CHAPTER 6, PART 1
VULNERABILITY SCAN PROCEDURES

1 BACKGROUND

Global network connectivity is commonplace for information exchange and is crucial for conducting many everyday operations. However, the benefits can be overshadowed by the increase in network vulnerabilities. The number of Information Technology (IT) related incidents that have occurred in the past year, along with the increase and complexity of threats, requires that USDA take their security protection measures seriously. Networks and information technology resources are continually vulnerable to illegal/ malicious activity or exploitation by internal and external sources.

Vulnerability Scan Procedures are a critical component of the Overall Security Protection Plan within the Department. Regular IT inventories and vulnerability scans have proven to be an effective tool in combating IT incidents and exploits of USDA information assets. The purpose of this document is to establish the policy and procedures for the inventory and vulnerability scans of all USDA managed networks, systems, and servers.

2 POLICY

All USDA agencies and mission areas will establish and implement the following procedures for accomplishing vulnerability scanning of all networks, systems, servers, and desktops for which they have responsibility. Each agency/mission area will report to CS all Critical Vulnerabilities (High and Medium) found as a result of the scan. Internet Security Systems (ISS) Internet Scanner software will be used to scan networks, systems and servers that will be obtained from the Department-wide Contract Vehicle established for this purpose. The ISS Software already classifies the vulnerabilities into high, medium and lows with default values from the vendor. Vulnerability Scans are to be performed on a monthly basis for all existing and new networks, systems, servers, and desktops by duly authorized users in accordance with established procedures. Cyber Security also requires that Discovery Scans be performed monthly to ensure that there are no “unauthorized devices” on agency networks.

Agencies will run scans inside USDA using USDA owned IP addresses, unless they have an approved exception to deviate from this policy. Physical or electronic inventories can be done of network, systems, servers, and workstations. However, electronic inventories are preferable. Each agency will designate authorized personnel to conduct software scans. All authorized users will be trained in the use of the scanner software prior to conducting any internal or external scans and will notify the CS before running scans. The National Intrusion Detection System (IDS) managed by CS detects all scans whether they originate externally or internally. Agencies/staff offices will identify the range of Internet Protocol (IP) addresses to be scanned and the IP address of the platform being used to launch the scan. Agencies and staff offices will not attempt to scan networks, systems, servers or desktops for which they are not responsible.

Agencies and staff offices will produce and retain inventory and vulnerability scan reports for all scans conducted in compliance with agency record management guidelines. The Monthly Scan Certification form, Appendix B, will be completed by the agency ISSPM and sent to CS at the end of each month. Critical vulnerabilities are those that have the potential to disrupt the operation of networks, servers and desktops used to transport USDA data. A summary of the vulnerabilities identified will be provided to the agency Chief Information Officer (CIO) for review to ensure that corrective action plans are developed within 30 days and implemented for critical vulnerabilities identified. A Plan of Action and Milestones (POA&M) will be developed in according with Federal Information Security Management Act (FISMA) reporting requirements for any unresolved critical vulnerabilities existing for more than 30 days from the date of the scan. Agencies do not need to request exceptions for "false positives".

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a

updated timeline for completion. CS will monitor all approved exceptions.

3 RESPONSIBILITIES

a The Associate Chief Information Officer for Cyber Security will:

(1) Provide customer support to agencies and staff offices in obtaining Internet Security Scanners, Scanning Software and Keys from the USDA Enterprise License Contract.

(2) Assist agencies/staff offices in obtaining training on the use of scanning equipment on their networks, systems, and servers;

(3) Provide technical guidance in scanner use to agencies and staff offices, as required, after training of authorized users has taken place;

(4) Conduct oversight reviews of agencies and staff offices to review vulnerability reports and corrective actions taken to ensure that networks, systems, and servers are protected in accordance with this policy; CS also reserves the right to review Discovery Scans;

(5) Monitors Scan Certification forms to ensure that agencies and staff offices comply with this policy; and

(6) Review all exceptions requesting exceptions to this policy in a timely manner and coordinate the response to the agency with the Associate CIO for IRM.

b The Associate CIO for Information Resources Management (IRM) will:

(1) Support the policy and procedures contained in this chapter to ensure that appropriate security protection is provided to all USDA managed networks, systems and servers; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security to any exception requests for exceptions to this policy.

c Agency Chief Information Officer will:

(1) Implement and enforce this policy and procedures within all internal agency/staff office activities who are responsible for network, systems, workstations, and servers;

(2) Ensure that all agency/staff offices order and use the Internet Security Scanner software and keys in conducting internal and external scans on a monthly basis and that inventories of networks, systems, servers, software and Internet Protocol (IP) addresses are maintained;

(3) Designate and notify CS of personnel authorized to conduct agency/staff office scans; ensure that these personnel are trained; notify Cyber security prior to conducting any scans;

(4) Review Scan Certification information on a monthly basis to ensure that critical vulnerabilities identified are corrected in a timely manner;

(5) Provide a completed Scan Certification Report (Appendix B) to CS for all agency systems and desktops scanned on a monthly basis;

(6) Submit a exception package, including a strong justification, for all critical vulnerabilities when corrective actions are not taken and forward to the Associate CIO for IRM for review and action; and

(7) Take necessary action to archive IP addresses, IT equipment inventory and vulnerability reports in compliance with agency records management guidelines.

d The agency Information Systems Security Program Managers (ISSPM), Systems/Network Administrators or Authorized Users will:

(1) Assist in performing monthly inventories and vulnerability and discovery scans of all agency/staff office managed networks, systems, workstations, server, and desktops as the authorized user;

(2) Assist in performing vulnerability scans of all new systems, network, or servers prior to production deployment and to existing systems after major changes are made;

(3) Assist in producing/updating inventory and vulnerability reports for all agency/staff office managed networks, servers, software and IP addresses on a monthly basis;

(4) Complete the Scan Certification (Appendix b) on a monthly basis for all agency systems and desktops;

(5) Forward the report to the agency Chief Information Officer for review and further action; and

(6) Document the status of actions taken by all Authorized Users to mitigate vulnerabilities identified or prepare a written exception package with a strong justification to agency/staff office IT Manager/CIO for actions not taken.

(7) Update quarterly POA&Ms in accordance with Federal Information Security Management Act (FISMA) reporting requirements with any unresolved critical vulnerabilities existing for more than 30 days from the date of the scan.

e Agency System/Network Administrators (not Authorized Users) will:

(1) Deploy new systems into production or operational status only after critical vulnerabilities are resolved through security mitigations or accreditation by the Designated Accrediting Authority (DAA)/agency CIO;

(2) Apply patches or fixes to agency/staff office managed networks, systems, servers, and desktops in a timely manner as appropriate;

(3) Keep a written record of all patches and fixes applied to agency/staff office managed networks, systems, and desktops, including the version and date; Cyber Security reserves the right to verify all written records of system/network/server patches;

(4) Collaborate with the ISSPM/Authorized Users in ensuring that IP Address updates, inventory of IT equipment and vulnerability scans are conducted/updated on a monthly basis; and

(5) Assist the ISSPM/Authorized Users in ensuring that mitigation actions are taken promptly for all critical vulnerabilities or that a persuasive and cogent written justification is provided to agency CIO for actions not taken.

-END-

Appendix A

Internet Scanner 7.0 User's Guide

July 20, 2004

Prepared by:
Craig J. Chase, Cyber Security Administrator
1400 Independence Ave, SW, Room 555 Reporters
Stop 7611
Washington, DC 20250
202-690-0271
craig.chase@usda.gov

Overview of Internet Scanner

Introduction

Internet Scanner is a vulnerability assessment product that analyzes the security of devices on an enterprise-wide network, checking for vulnerabilities on routers, Web servers, Unix servers, and Windows servers, desktop systems, and firewalls.

Internet Scanner can be used on all TCP/IP-based networks, networks connected to the Internet, and on stand-alone networks and machines.

This user's guide will provide the basic steps in the basic installation and operation of the Internet Scanner 7.0. If you require more detailed information, please refer to the PDF document entitled "Internet Scanner User's Guide", provided by Internet Security Solutions (ISS).

Benefits of Internet Scanner

There are many benefits that Internet Scanner provides. Some include:

- Internet Scanner performs the widest variety of vulnerability detection, ranging from gathering information to finding vulnerabilities.
- Internet Scanner finds vulnerabilities much as an intruder would, by examining network devices, services, and interrelationships.
- Internet Scanner provides detailed information about each vulnerability, such as the vulnerable host, description, and corrective actions.
- Internet Scanner also provides different levels of reporting for different audiences, such as illustrated management reports. Other reports include the Summary and Detailed Host Vulnerability reports for administrators.

Internet Scanner Architecture

Internet Scanner is divided into two areas of functionality:

- The Console – a collection of tools used to control the Internet Scanner Sensor locally. It also provides stand-alone reporting and policy editing.
- The Sensor – scans devices connected to the network by using vulnerability checks that attempt to detect known security issues.

The Internet Scanner Console

There are seven major components of the Internet Scanner console. They are:

Component	Description
Client – Scanner GUI *Scanner_Console.exe*	Controls the sensor and scan options from a GUI front end.
Client – 7.0 CLI/Engine Manager *EngineMgr.exe*	Controls the sensor and multiple scan options from the command line for scheduling and scripting.
Client – 6.2.1 CLI *ISS_WinNT.exe*	Provides backward compatibility to support custom scripts written to control older versions of Internet Scanner.
Policy Editor *CPE.exe*	Used to customize policies.
Policy Migration *PolicyMigration.exe*	Used to migrate custom policies from Internet Scanner 6.2.1
X-Press Update Installer *XpressUpdate.exe*	Used to download and install updates to the current version of Internet Scanner
Report Engine *ReportEngine.exe*	Runs reports in various formats based on vulnerability scans.

The Internet Scanner Sensor

There are six major components of Internet Scanner Sensor. They are:

Component	Description
Scan Controller *ISSDaemon.exe*	Directs job requests to the appropriate sensor components.
Database *Scan7db.mdf*	Stores scan results
Flex Checks *FlexCheck.exe*	The engine responsible for running custom vulnerability checks.
Discovery *Discovery.exe*	The engine responsible for enumerating live hosts.
OS Identification *Discovery.exe*	The engine responsible for identifying remote operating systems. Part of Discovery.
Assessment Checks *Builtin MicroEngine.exe* *Plugin MicroEngine.exe*	Engines responsible for checking for specific vulnerabilities.

SiteProtector and Distributed Scanning Solutions

Internet Scanner incorporates native support of SiteProtector, and allows Internet Scanner to be centrally managed. USDA's enterprise licenses for Internet Scanner also includes the SiteProtector license. Please contact your ISSPM for a license key.

This user guide does not cover using SiteProtector with Internet Scanner. For more information on Site Protector and Internet Scanner, please see the "Internet Scanner User's Guide", provided by ISS.

Installing Internet Scanner

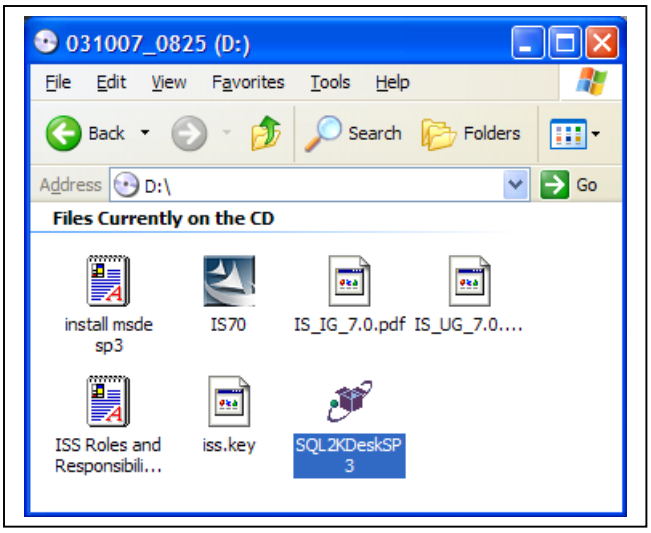
Requirements for Installation

These items are required when installing Internet Scanner.

Item	Minimum Requirement
Processor	600 MHz Pentium III
Operating System	• Windows NT 4.0 Workstation with Service Pack 6a SRP • Windows 2000 Professional with Service Pack 3. • Windows XP Professional Service Pack 1 The installation of Internet Scanner is not supported on Windows NT 4.0, Windows 2000 or Windows 2003 servers.
Other software	• Microsoft Internet Explorer 5.5 SP2 or later required to run HTML Help. • Adobe Acrobat Reader 4.x or later is required to view the PDF files in the Manuals folder. • For reporting purposes, a printer driver is required on the computer running Internet Scanner. The Generic/Text only printer driver is sufficient.
Memory	256 MB
Hard disk	• 315 MB for installation from CD ROM • 345 MB for installation from file. NTFS file partition required.
User privileges	Local or domain administrator.
Database	Microsoft SQL Data Engine (MSDE) 2000 Service Pack 3.
Microsoft MDAC	Version 2.7

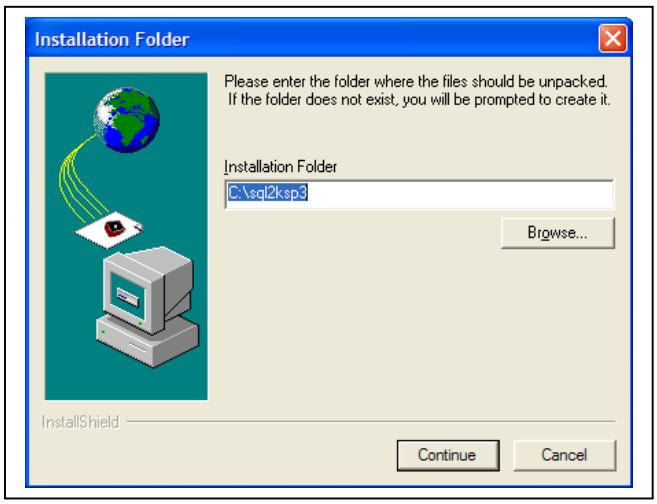
Steps for Installing of Microsoft SQL 2000 Desktop Engine (MSDE)

Step 1: From the CD, Shared Drive or your hard drive, double-click on the **SQL2KdeskSP3a.exe** exe icon to launch program.



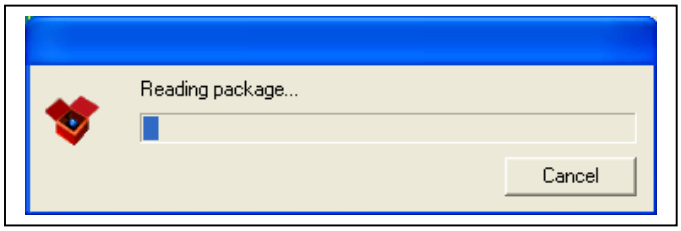
Step 2:
Click "**I Agree**" under the license agreement.

Step 3:
Choose an installation folder. Default is **c:\sql2ksp3**. Click **Continue** when finished.



Step 4:
For "The specified folder does not exist. Create it?" Click **Yes.**

You should see the installation process proceed with this window.



Step 5:
After installation is complete, please to go a command prompt or MS-DOS prompt. You can reach this by going to **Start|Run**, and type "**cmd**" in the open window.

Step 6:
Once at command prompt, please **type**:

```
C:\>cd sql2ksp3

C:\sql2ksp3>cd MSDE
```

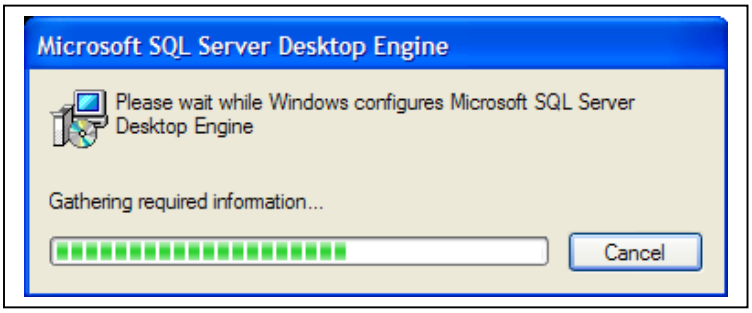
This changes the directory to c:\sql2ksp3\msde

Step 7:
In this step, you will need to setup MSDE with a system administrator password. The example below shows the syntax in defining the system administrator password as “password01”. Replace “password01” to a unique alphanumeric complex password.

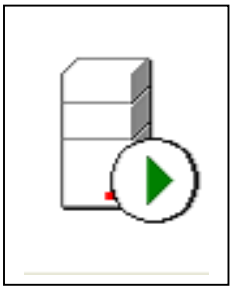
At C:\sql2ksp3\msde, **type**:

```
sql2ksp3\MSDE>setup.exe sapwd=password01
```

You should see a window that is installing MSDE much like this one:



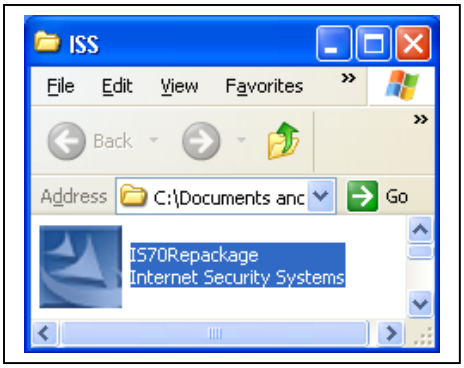
Step 8:
Once window disappears, please reboot machine. After reboot, you should see an icon in the System Tray similar to this:



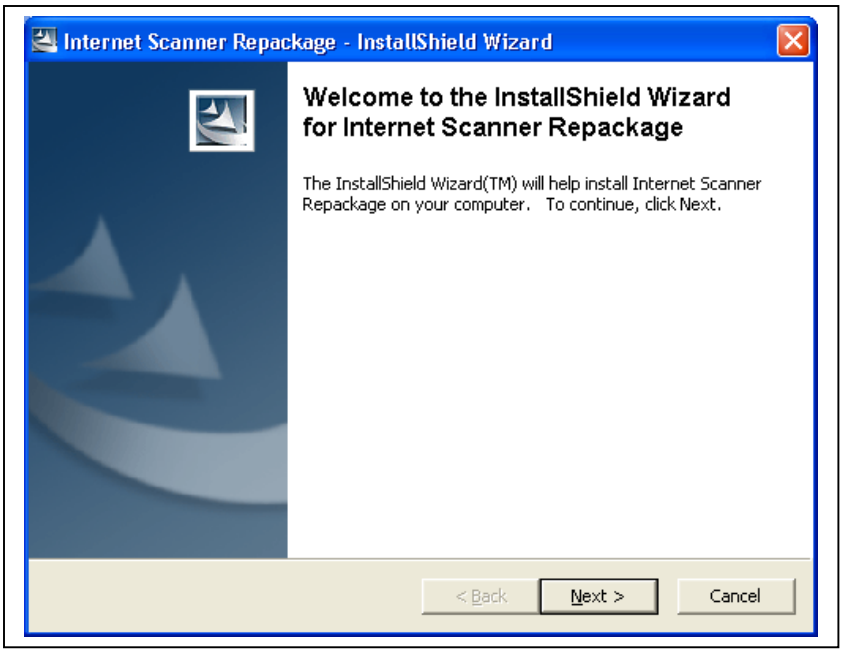
For more information on installing MSDE, please refer to ISS Knowledge Base Article 1918 at http://www.iss.net/**.**

Steps for Installing Internet Scanner 7.0 Repackage

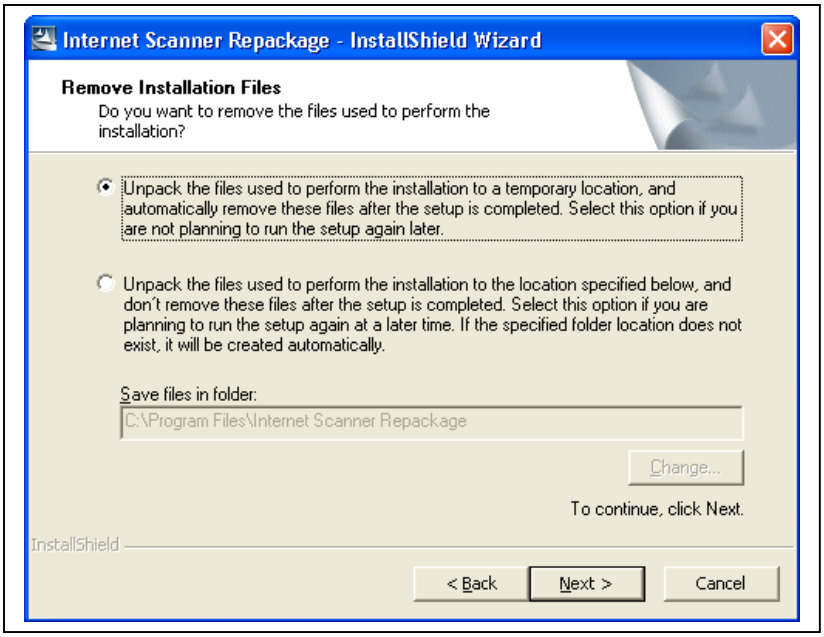
Step 1:
From the CD, Shared Drive or your hard drive, **double-click** on IS70Repackage.exe



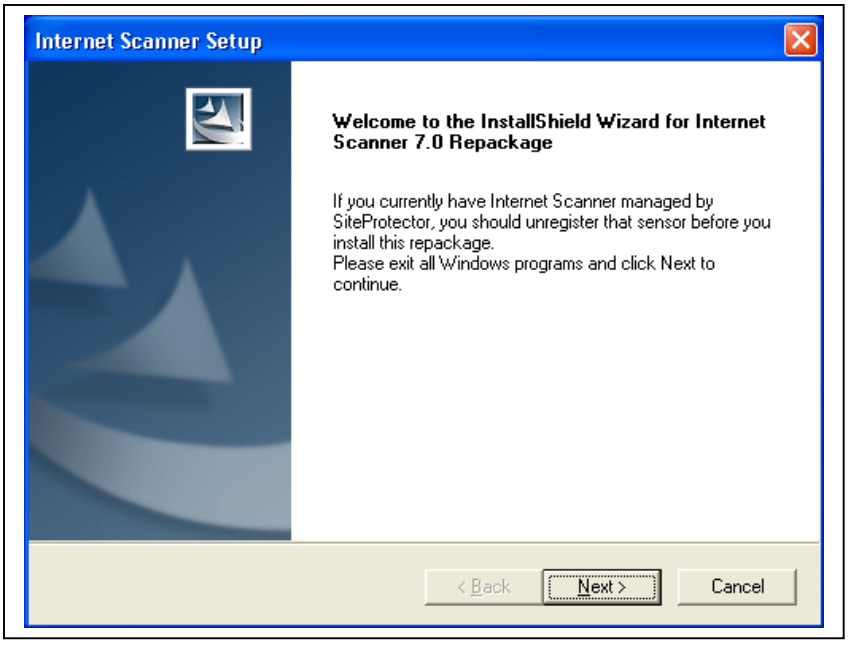
Step 2:
Internet Scanner will start the installation process. Click **Next** to continue.



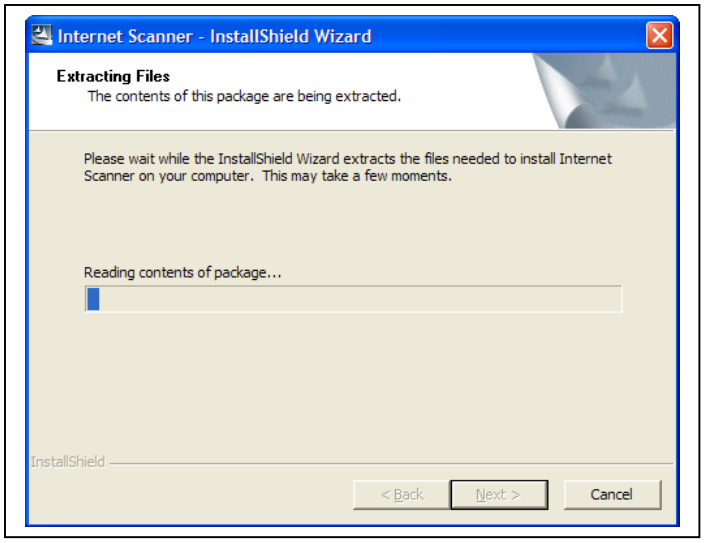
Step 3:
The Remove Installation Files window appears. **Select** Unpack the files used to perform the installation to a temporary location, and automatically remove these files after the setup is completed. Select this option if you are not planning to run the setup again later. Click **Next** to continue.

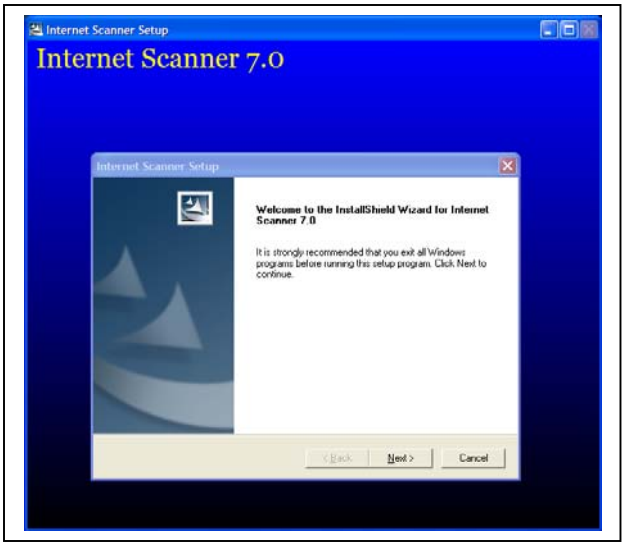


Step 4:
The Internet Scanner Setup window appears. Click **Next** to continue.

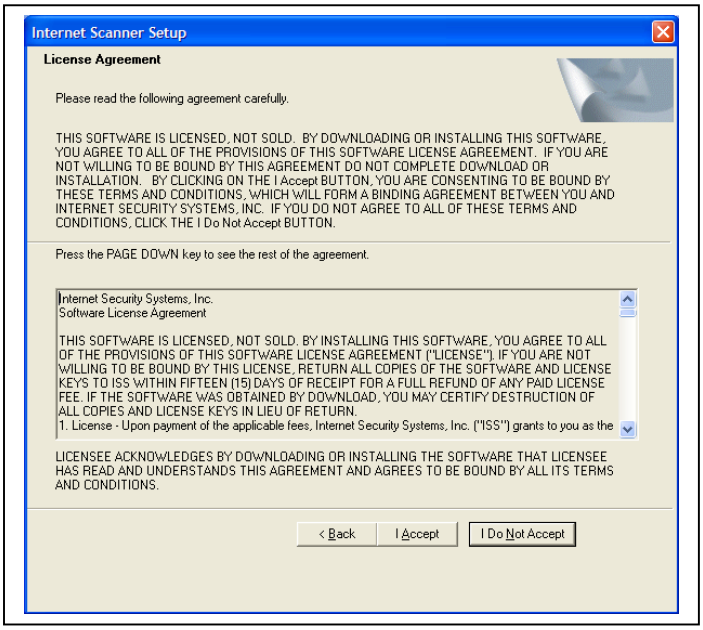


Step 5:
The installation will continue. Click **Next** to continue.

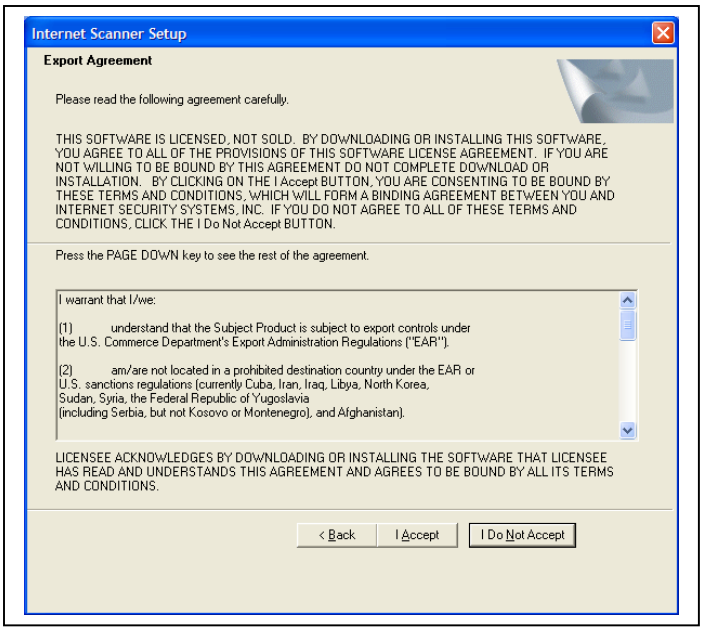




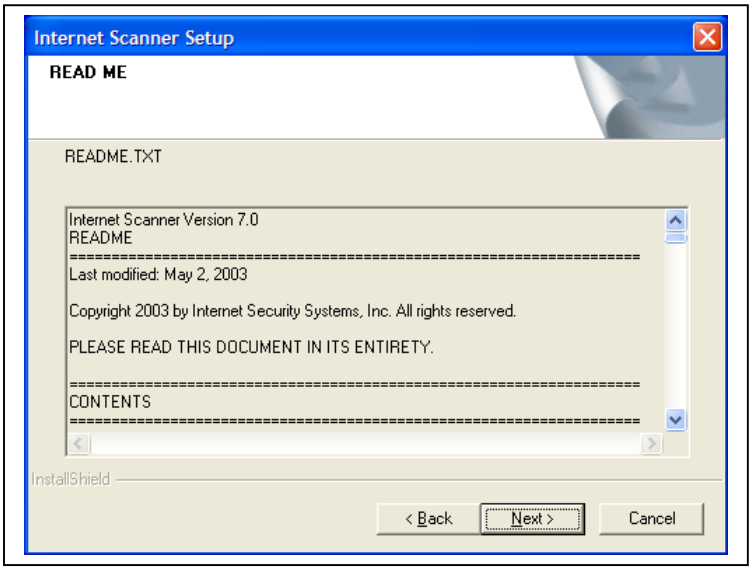
Step 6:
Click "**I Accept**" to accept the license agreement.



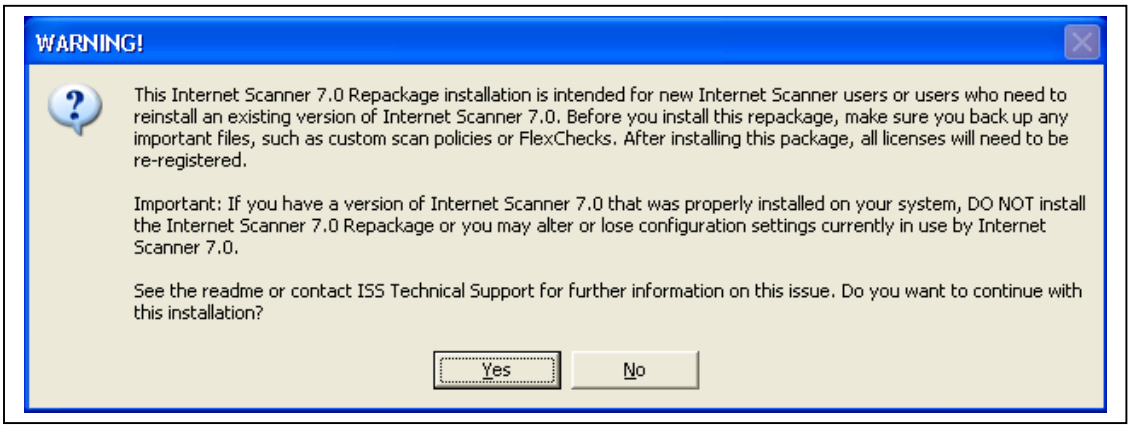
Step 7:
Click **"I accept"** to the export license agreement.



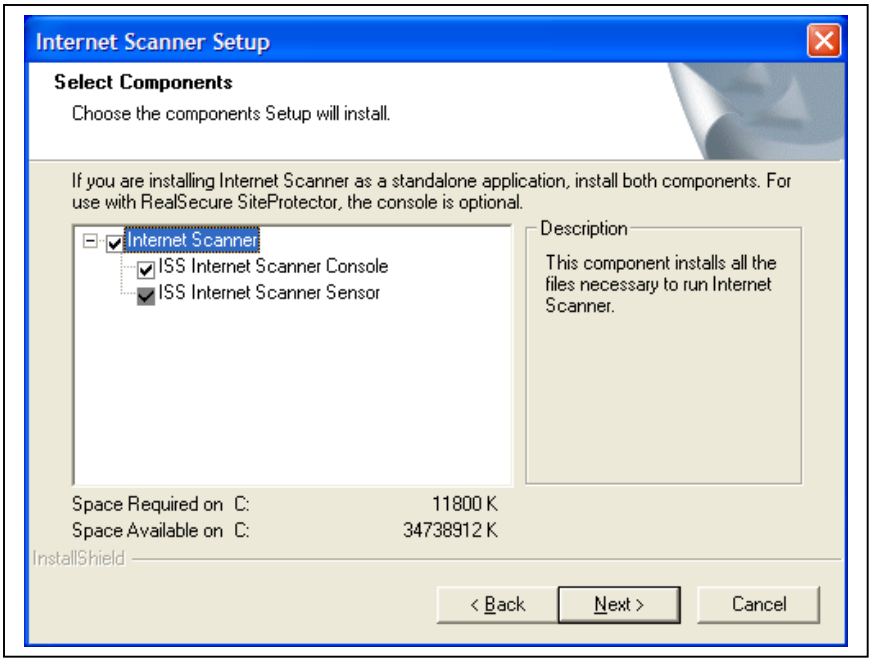
Step 8:
After viewing the readme text, click **Next** to continue



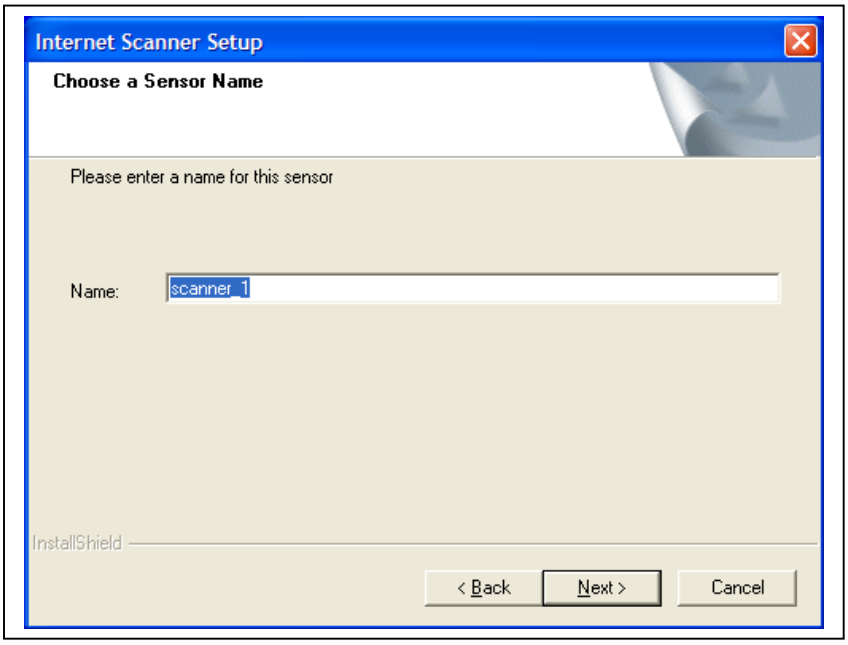
Step 9:
The Warning window appears. Please read message, and select **Yes** to continue.
Note: The Internet Scanner Repackage Installation is intended for new installations, or for users who need to reinstall versions of Internet Scanner as a result of technical problems. If you have a current installation of Internet Scanner 7.0, and the software is functioning normally, do not install Internet Scanner 7.0 Repackage software. Please contact ISS technical for more information.



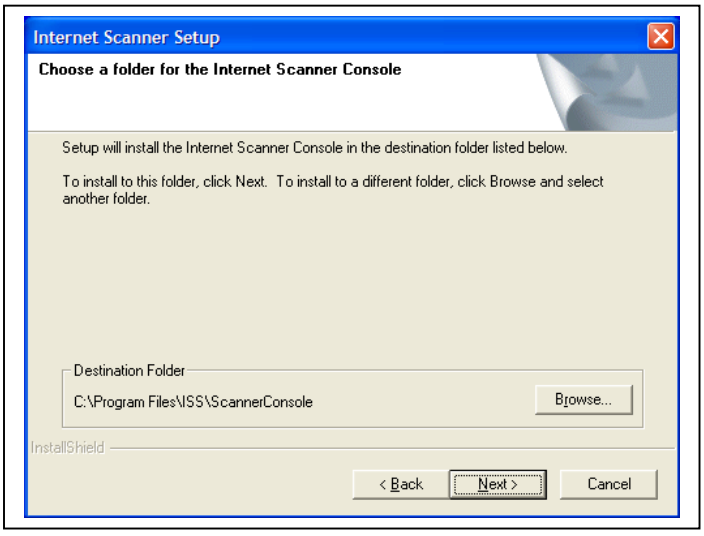
Step 10:
Under "Select Components", accept default settings and click **Next.**
Note: A standalone Internet Scanner software installation requires both ISS Internet Scanner Console, and Internet Scanner Sensor. If you are running Internet Scanner with RealSecure SiteProtector, the installation of the Internet Scanner Console is optional. Please refer to the "Internet Scanner User's Guide" by ISS.



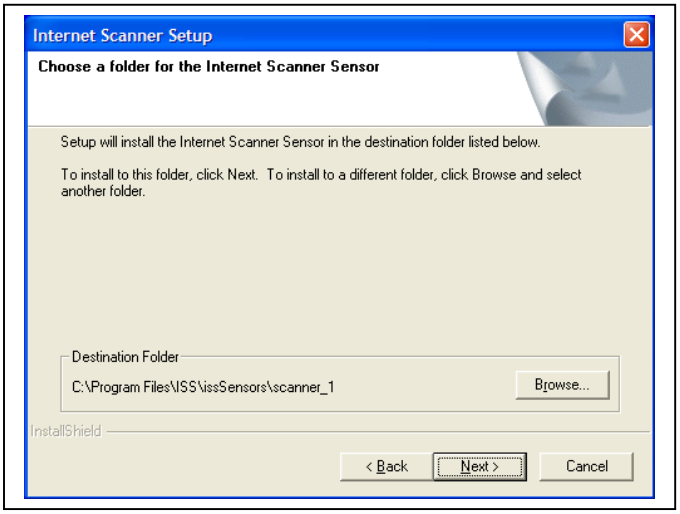
Step 11:
Under “Choose Sensor Name”, leave default name “**scanner_1**” and click **Next.** This feature is for the Engine Manager Command Line Interface, and for use with RealSecure SiteProtector.



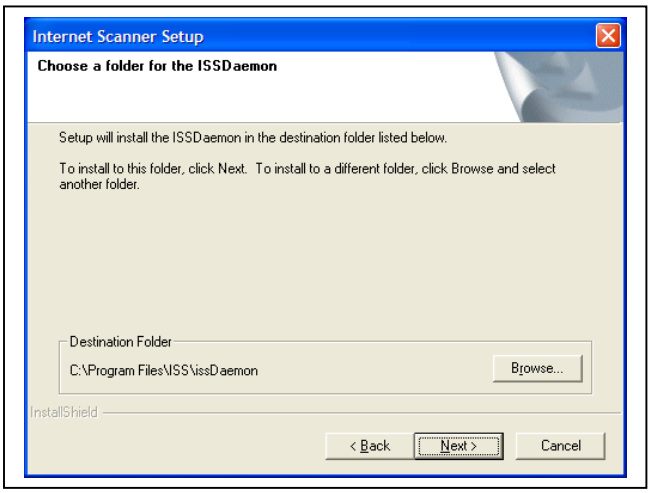
Step 12:
Accept the default setting to install Internet Scanner Console. Default setting is: **C:\Program Files\ISS\ScannerConsole**. Click **Next** to continue.



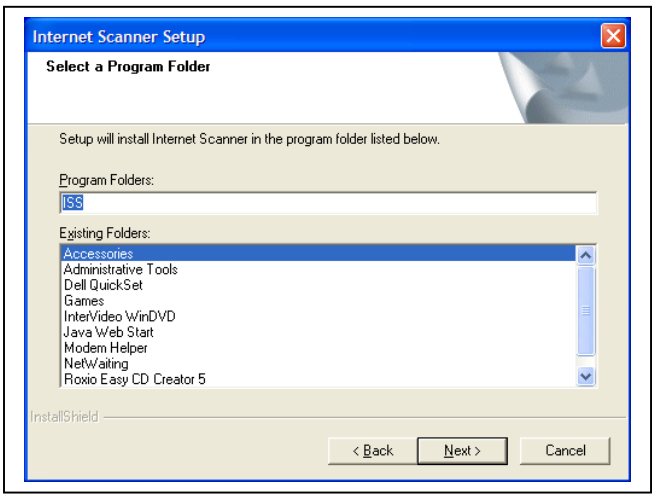
Step 13:
Accept the default setting to install Internet Scanner Sensor. Default setting is: **C:\Program Files\ISS\issSensors\scanner_1**. Click **Next** to continue.



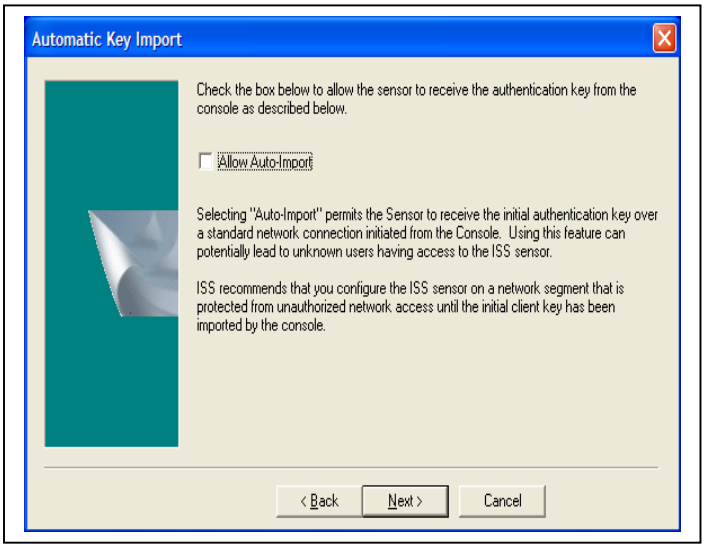
Step 14:
Accept the default setting to install the ISSDaemon. Default setting is: **C:\Program Files\ISS\issDaemon.** Click **Next** to continue.



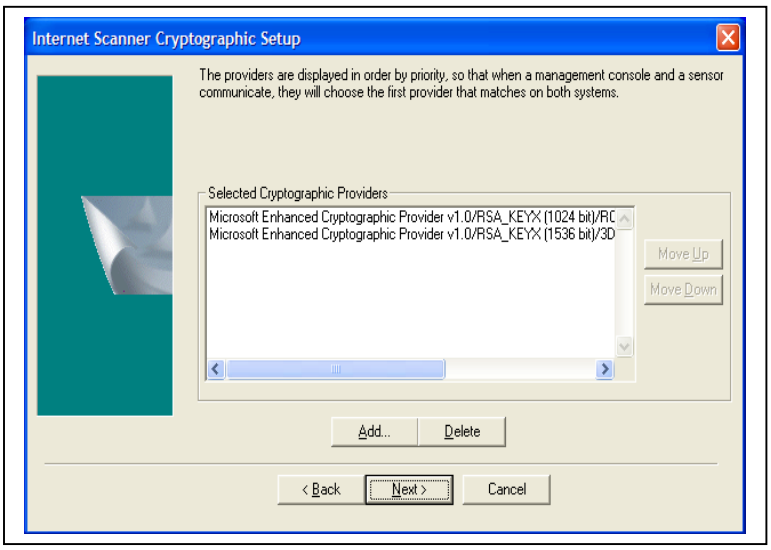
Step 15:
Under “Select a Program Folder”. Accept default setting “**ISS**” for program folder creation and click **Next.**



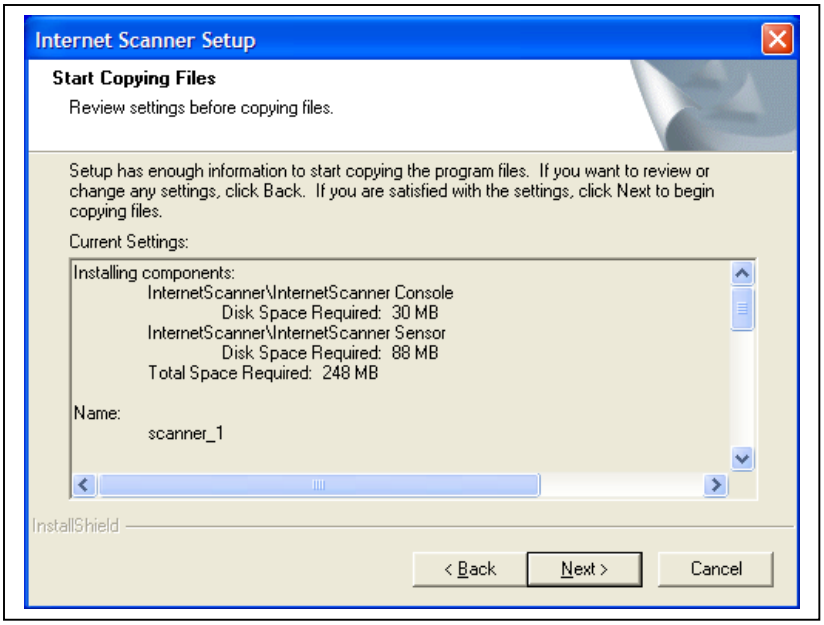
Step 16:
Deselect “**Allow Auto-Import**”. Click **Next** to continue.



Step 17:
The Internet Scanner Cryptographic Setup appears. Accept default configuration and click **Next.**



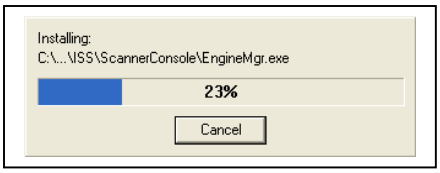
Step 18:
The review settings window appears. Verify settings and click **Next.**

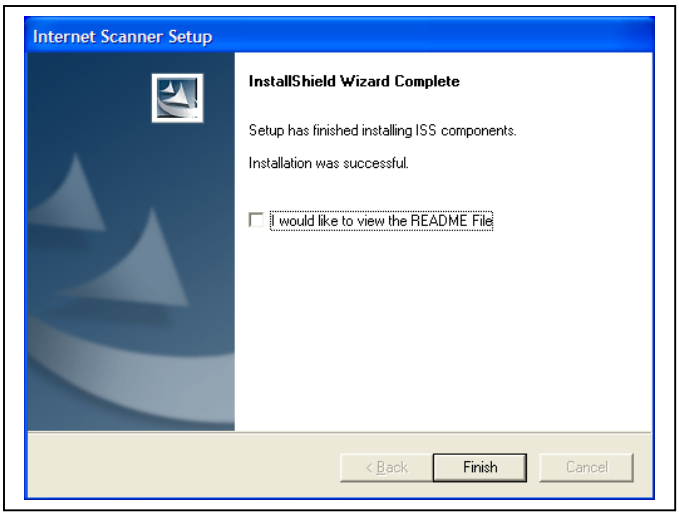


Step 19:
The Archive ISS Sensor Cryptographic Private Keys appears. Uncheck "**Archive the private keys**", and click **Next.**

Step 20:
The Archive ISS Console Cryptographic Private Keys appears. Uncheck "**Archive the private keys**", and click **Next.**

Step 21:
The installation will begin installing files onto your computer. You will see the following windows. Click **Finish** when completed.





Step 22:
You must reboot your computer after installation, even if it does not prompt you to restart your computer. **After reboot, run Windows Update.**

Using Internet Scanner

Software License and Key

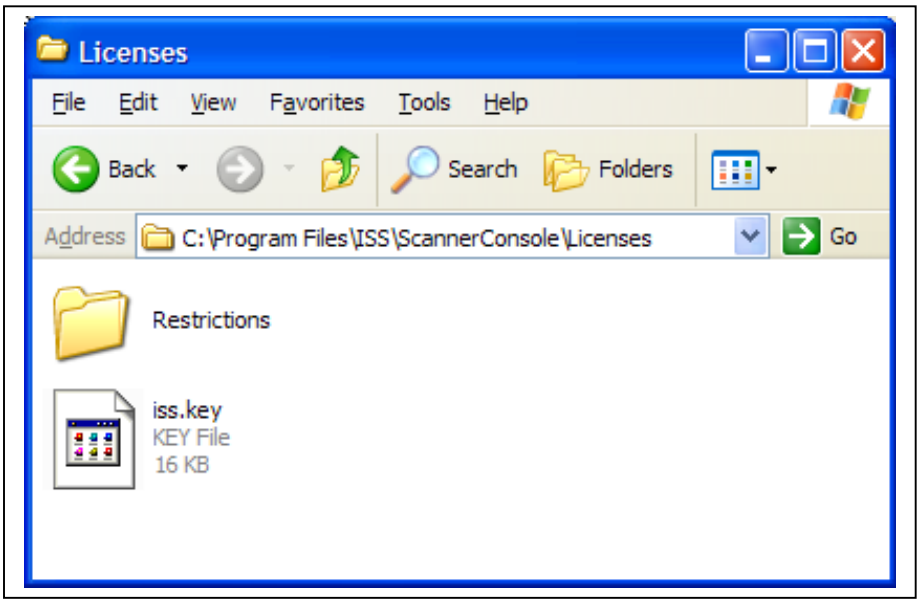
An Internet Security Systems Software license key is necessary for Internet Scanner to function properly. Without the iss.key file, the scanners cannot analyze activity across your network and on your computer system. Before you can use Internet Scanner, you must obtain and install your license key. Your Security Officer or ISSPM will most likely email you your license key as a Key File email attachment.

What is a Key File? A key file defines your licensing for Internet Scanner. It contains information such as the products licensed, creation date, maintenance expiration date, and license expiration date.

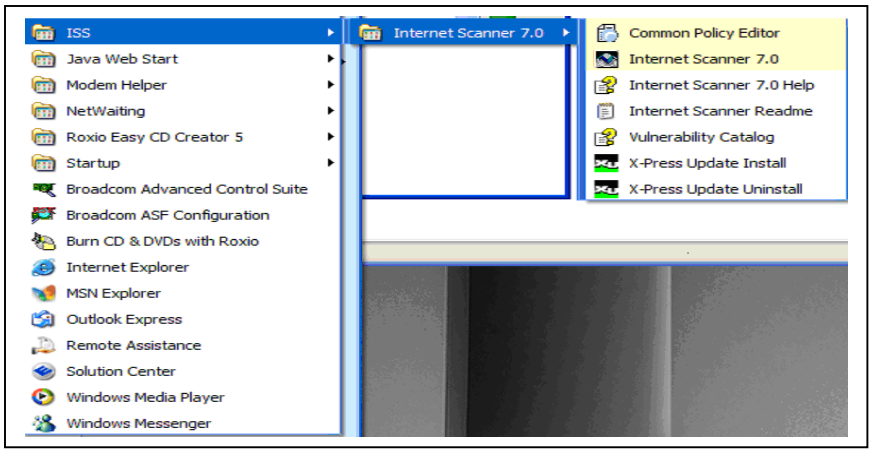
Note: With Internet Scanner version 7.0, you will be able to scan any valid IP address, regardless of the IP restriction in the license key. If you wish to restrict IP addresses to be run by Internet Scanner, you must deploy SiteProtector. Refer to the Internet Scanner 7.0 User's guide from ISS for more information.

Instructions for Installing the License

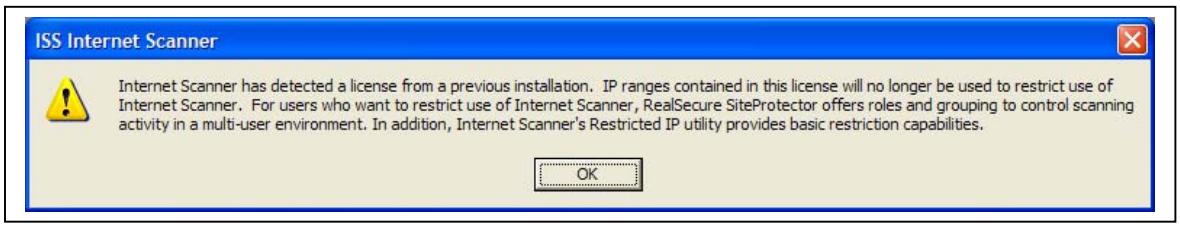
Step 1:
If you receive your Key File license through email, save the file using "**iss.key**" as the filename. Be sure to type the filename in double quotes, in order to avoid having your system apply some other extension to the file name. Save this file in **c:\program files\iss\scannerconsole\Licenses** directory.



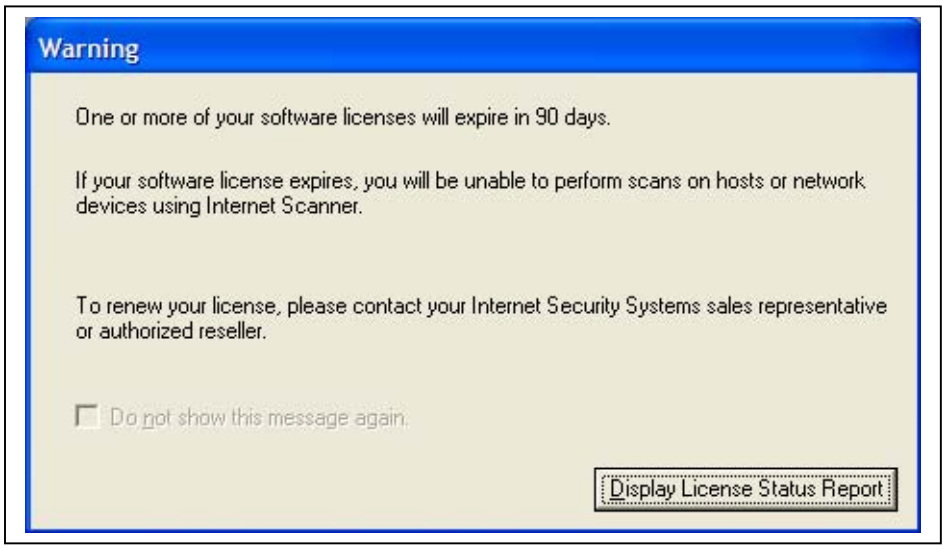
Step 2:
You must start Internet Scanner to finish installing and registering the key. To start Internet Scanner, Click **Start|Programs|ISS|Internet Scanner 7.0|Internet Scanner.** This will launch the Internet Scanner software.



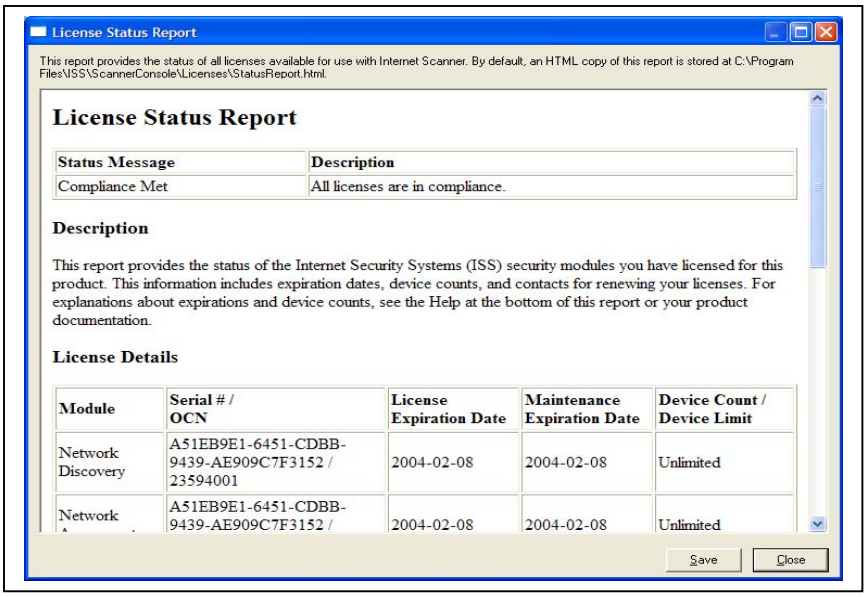
Step 3:
You should receive a message stating that Internet Scanner has detected a license from a previous installation. Click **OK** to continue.



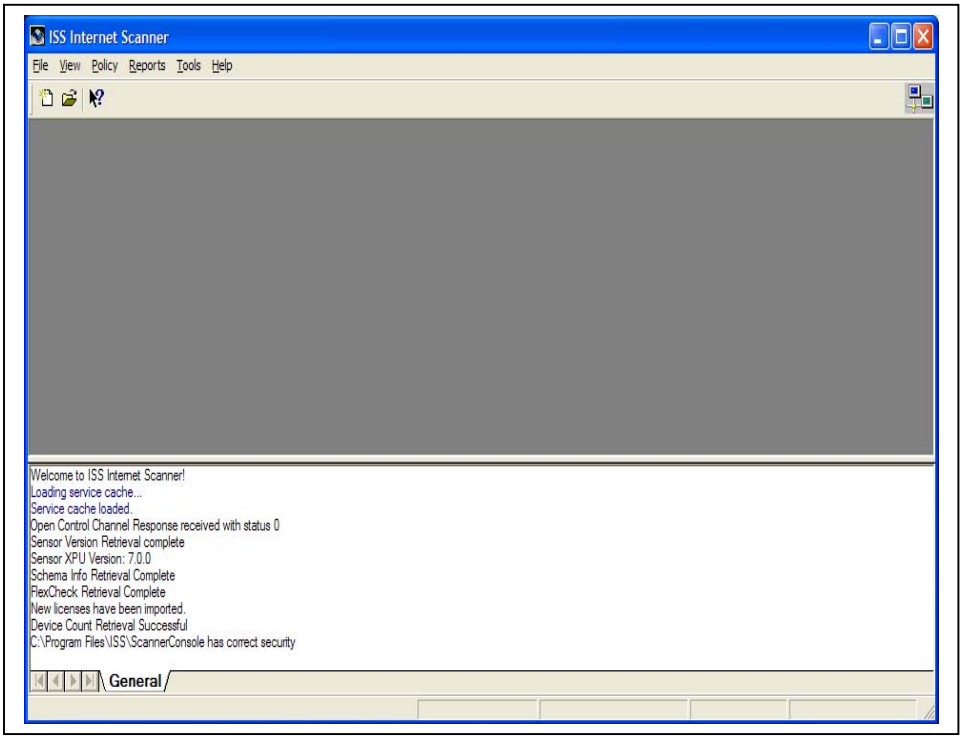
Step 4:
You may receive a warning message regarding your message license. Click "**Display License Report**".



Step 5:
The License Status Report window appears. Click **Close.**



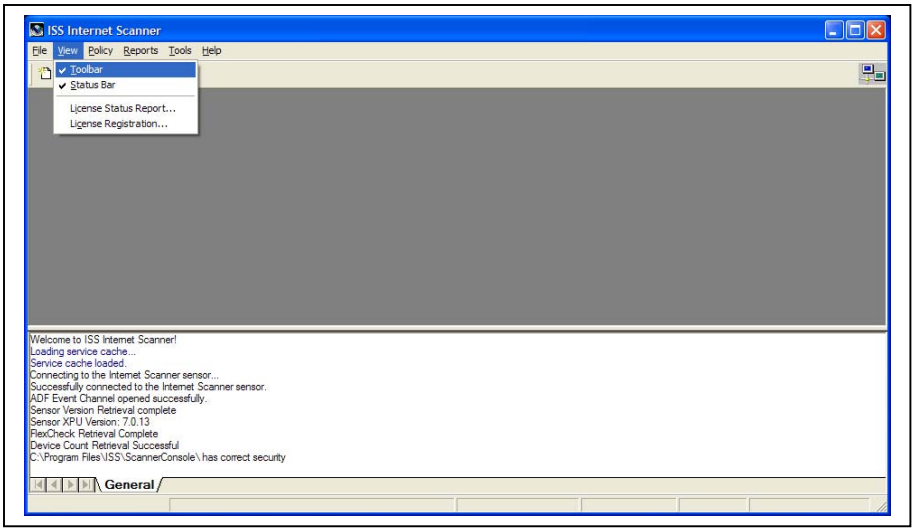
Step 6:
The Internet Scanner Console appears. When finished, exit out of the application and continue to X-Press Updates.



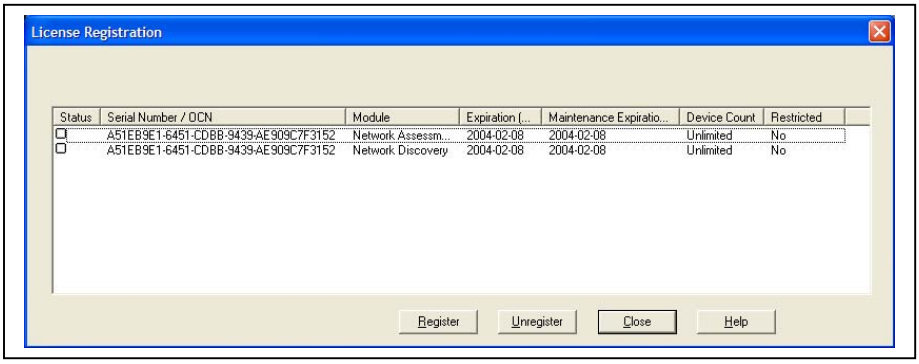
Instructions for Replacing an Expired License Key

There will be times where you will need to update your expired license key to a new license key. Unfortunately, Internet Scanner does not provide a seamless way to upgrade to a new license key. These steps will allow you to replace your existing license key to a new one.

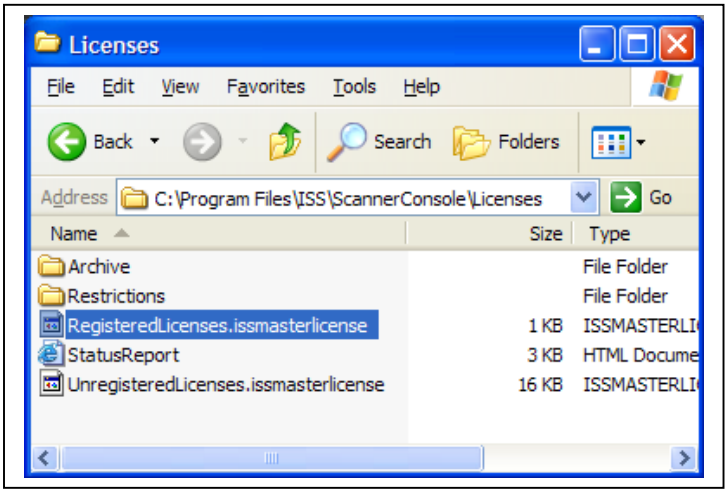
Step 1:
Open Internet Scanner 7.0. Once at the main screen, click **View|License Registration…**



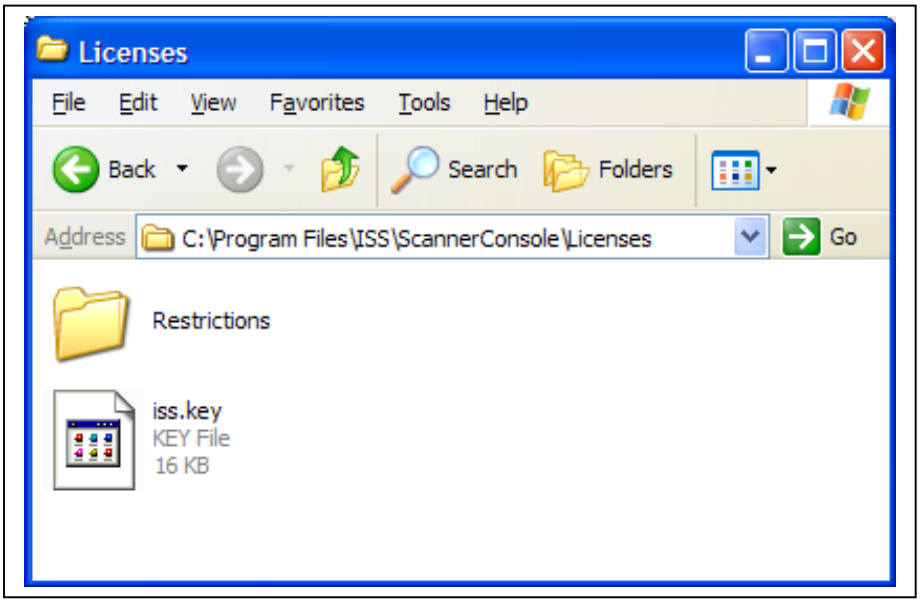
Step 2:
The License Registration window appears with a list of licenses. Click **Unregister** to unregister all licenses. An "X" should disappear under the Status column. Click **Close** when complete. **Exit** out of Internet Scanner.



Step 3:
Using Windows Explorer, go to **c:\program files\iss\scannerconsole\Licenses** directory. You should see two files titled "RegisteredLicenses.issmasterlicense" and "UnregisteredLicenses.issmasterlicense". **Delete** both files. **Delete** the Archive Directory.



Step 4:
Copy the "iss.key" to the same directory (**C:\program files\iss\scannerconsole\Licenses**). When complete, close all open windows and continue with **Step 2** under "Instructions for Installing the License".



X-Press Updates

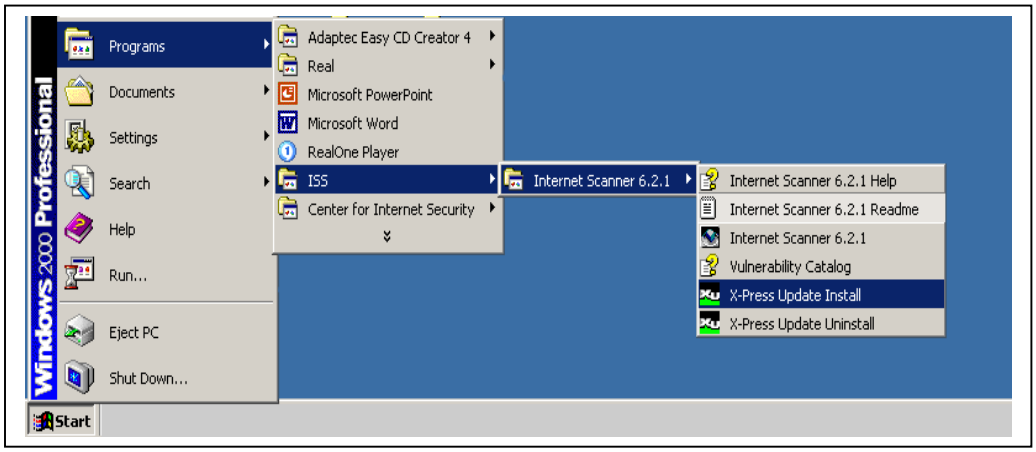
Introduction

X-Press Updates are packages of new security checks for Internet Scanner. They updates work much like virus updates for antivirus software. These updates are usually released on a monthly basis. Internet Scanner has an X-Press Update Installer program that checks for downloads and installs X-Press Updates. The installer can be run automatically as often as you wish.

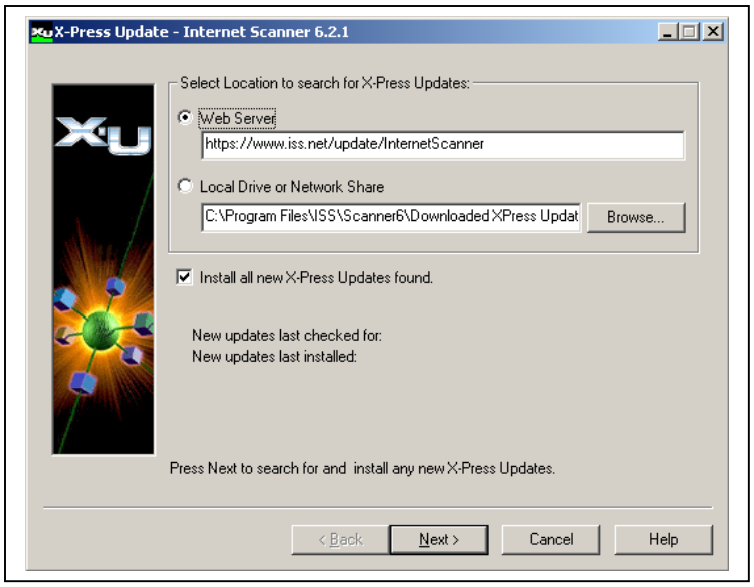
Running X-Press Updates

X-Press Updates automatically update your system with the latest checks and latest product updates available for Internet Scanner. To install new X-Press Updates not currently on your system, follow these steps:

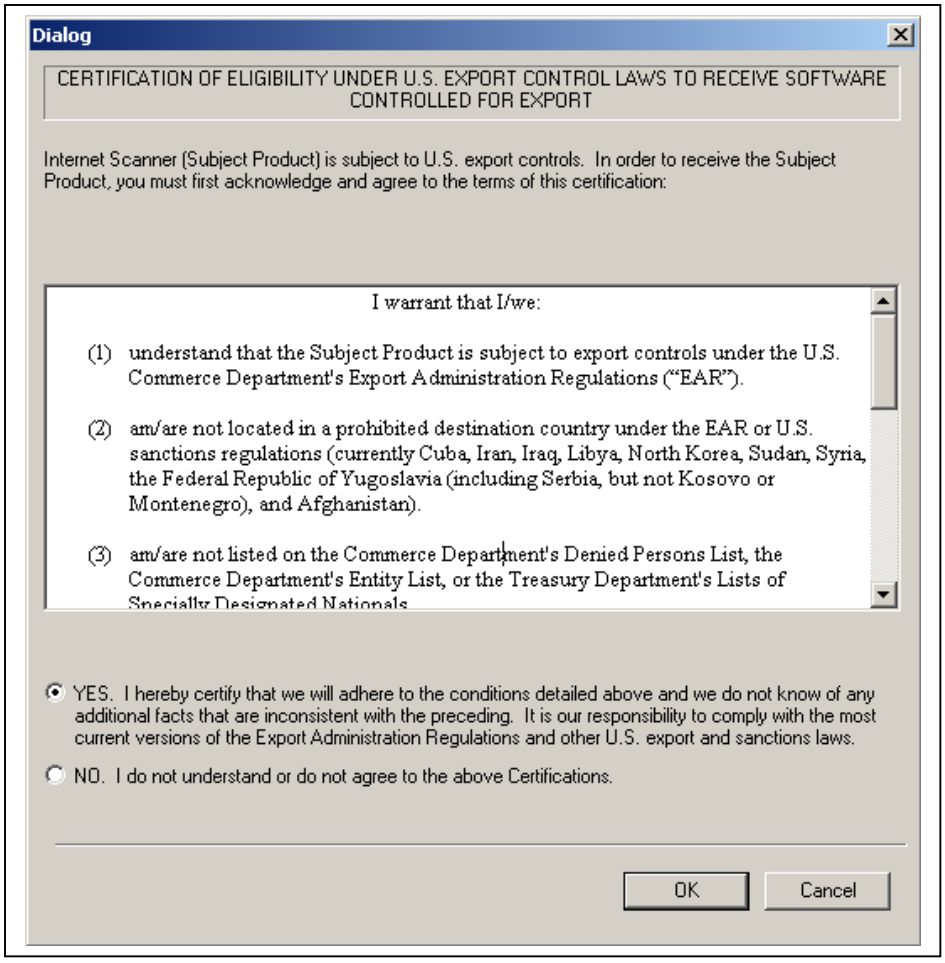
Step 1:
Click Start|Program|ISS|Internet Scanner|X-Press Update Install.



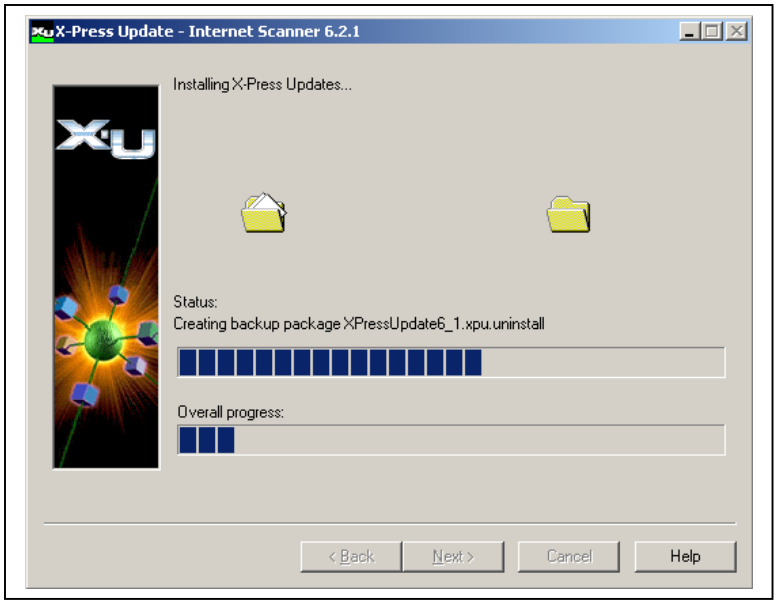
Step 2:
The Select Location window is displayed. **Select** Web Server option, and **Check** Install all new X-Press Updates found. Click **Next** to continue.



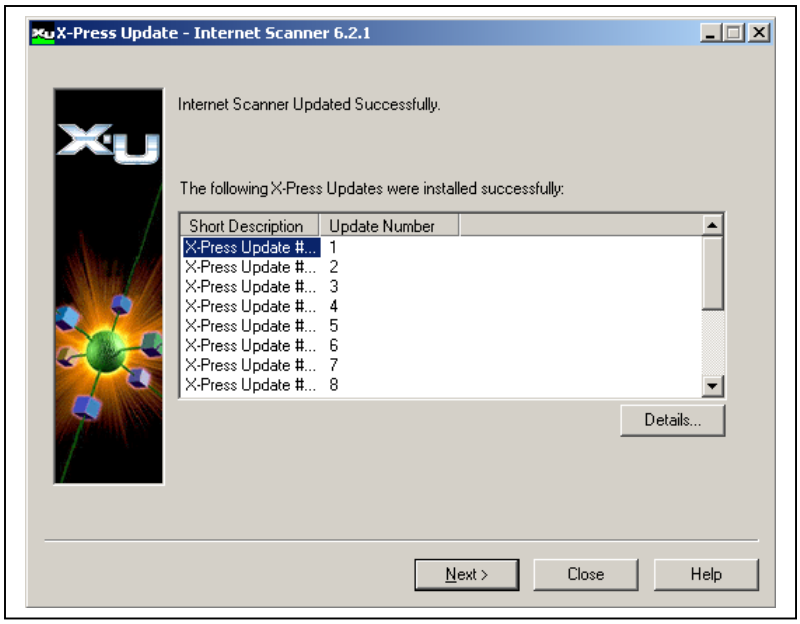
Step 3:
Select **Yes** to agree to the Export Law Agreeement, and then **Click** OK.



X-Press Updates will show the following status screen when updating.

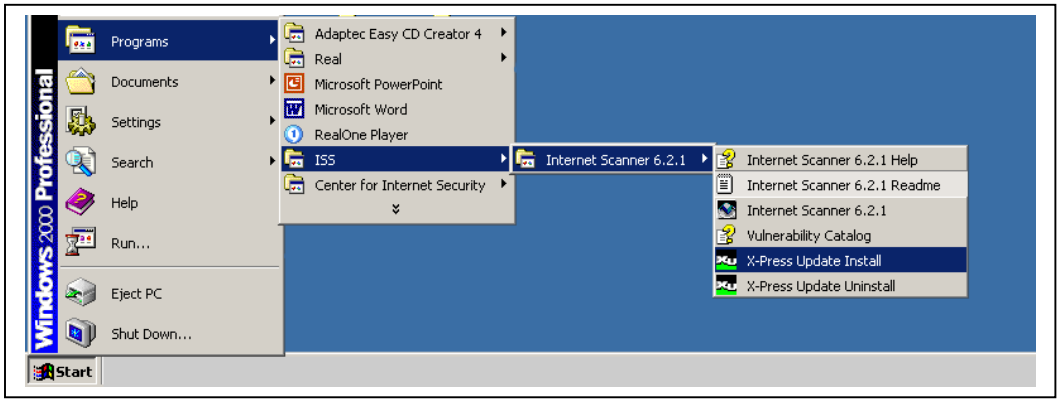


Step 4:
X-Press Update will show the following screen, when it has successfully completed.
Click Close to exit out the program.

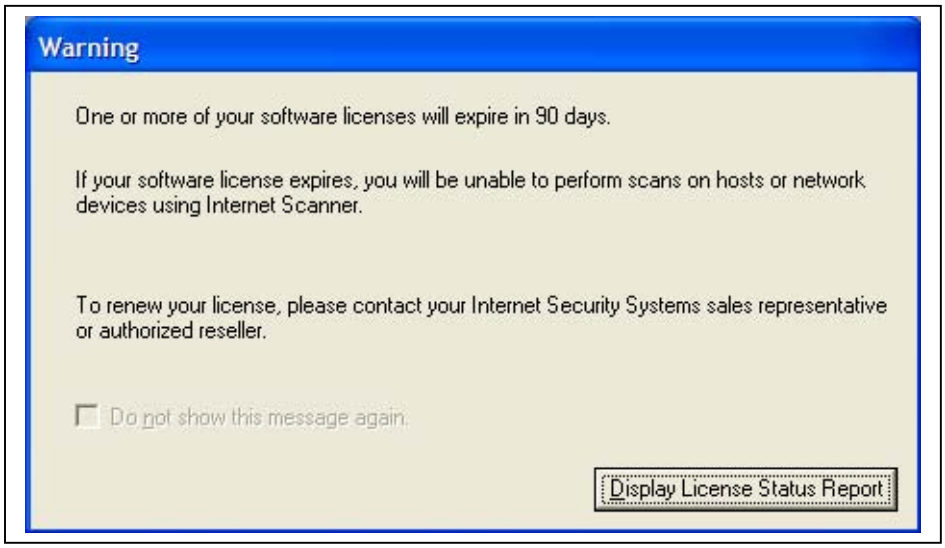


Running Internet Scanner

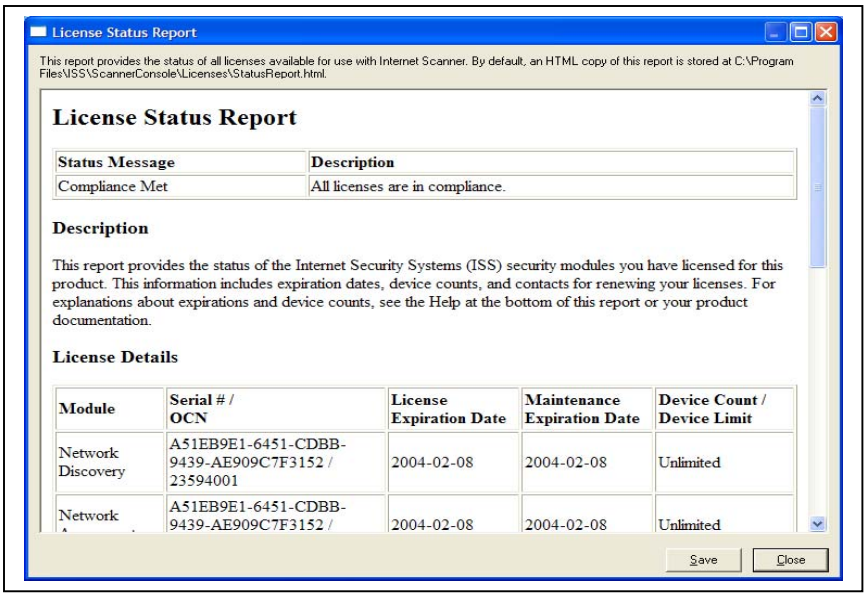
Step 1:
To start Internet Scanner, Click **Start|Programs|ISS|Internet Scanner 7.0|Internet Scanner.** This will launch the Internet Scanner software.



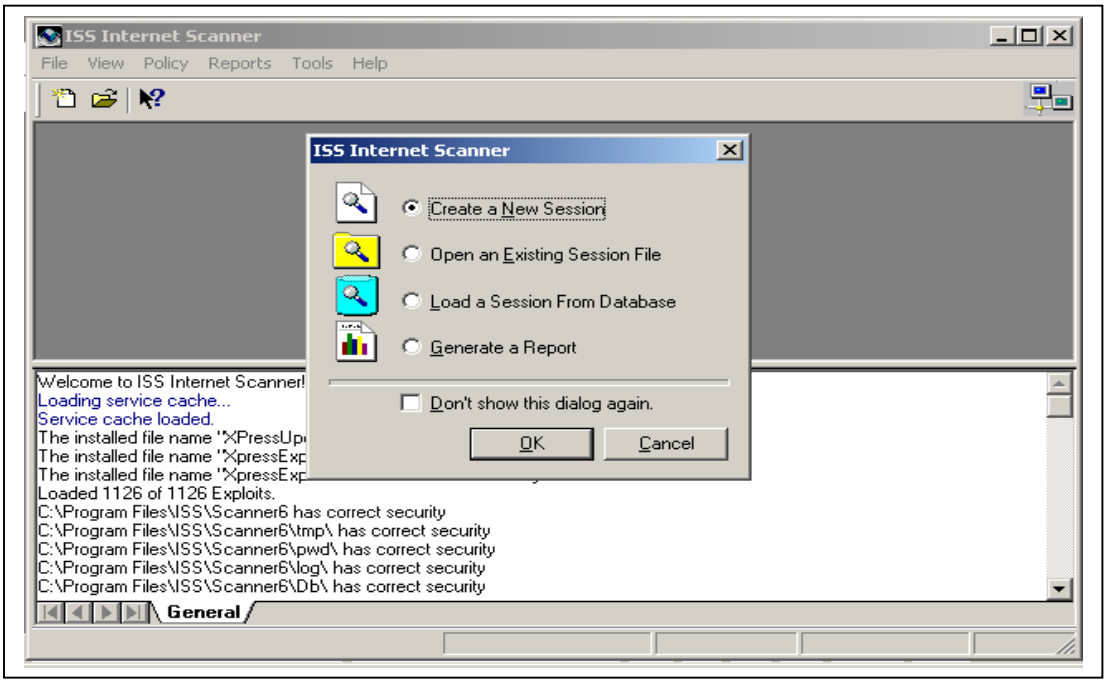
Step 2:
You may receive a warning message regarding your message license. Click "**Display License Report**".



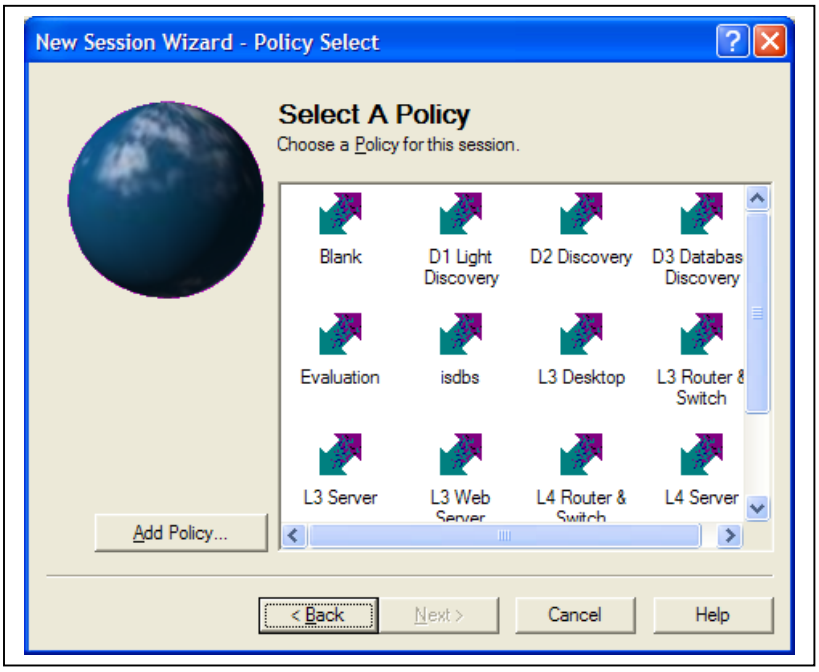
Step 3:
The License Status Report window appears. Click on **Close.**



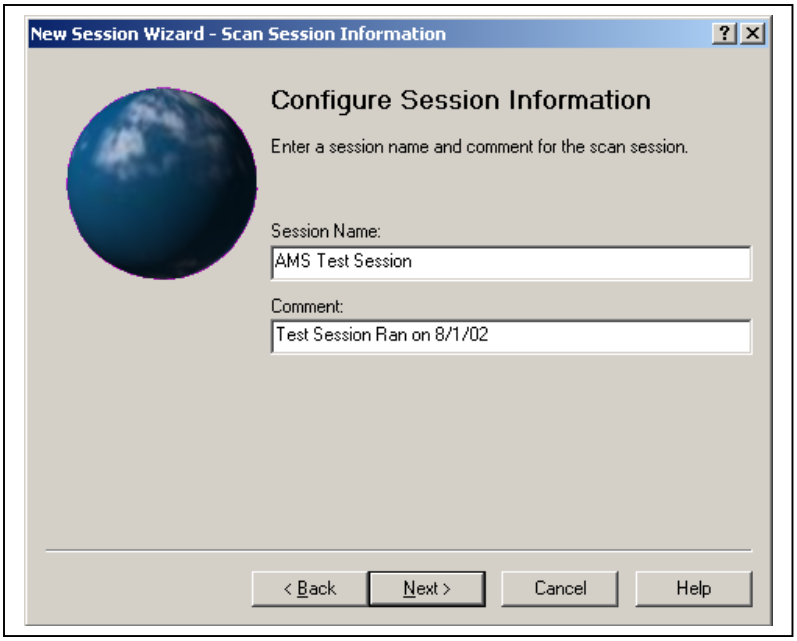
Step 4:
Select **Create a New Session** and Click **OK.**



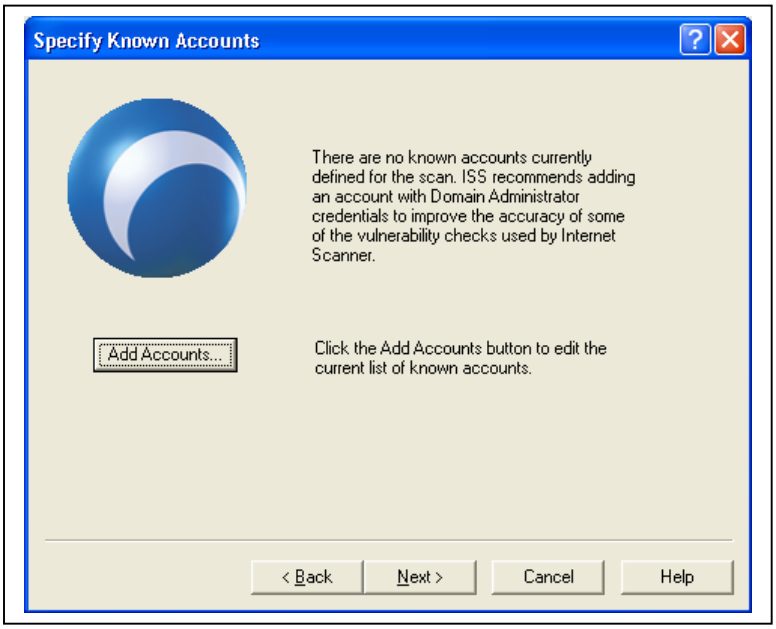
Step 5:
Select the policy that you wish to use, and Click **Next.** For a description of policies, please see “Identifying Security Levels and Policies in Internet Scanner” in the next session.



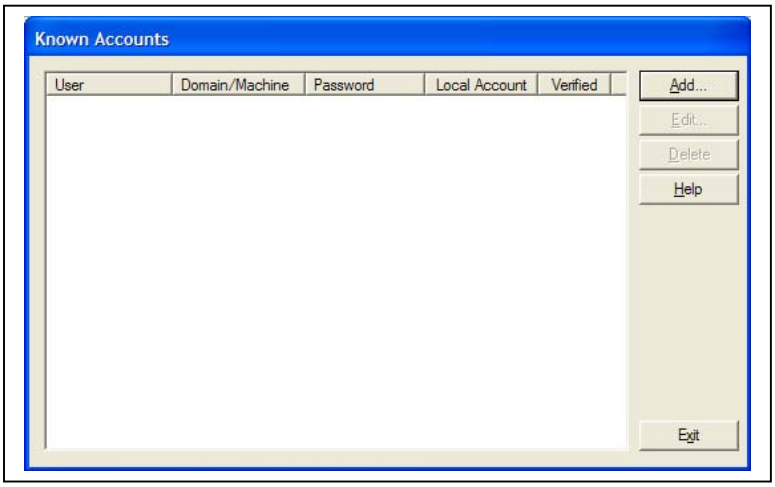
Step 6:
Type a session name and comment for the scan session and Click **Next.** This will be used to identify the sessions in the Internet Scanner database.



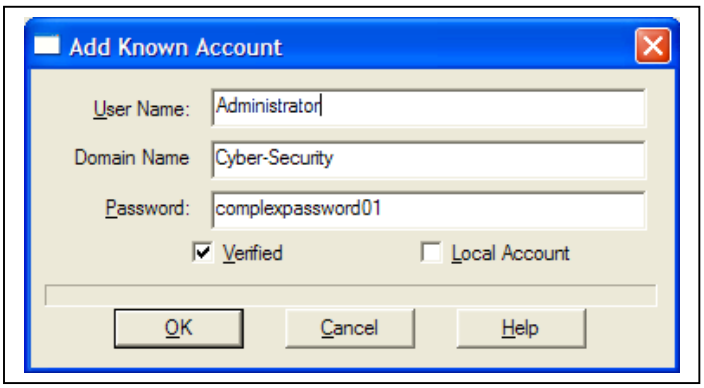
Step 7: The Specify Known Accounts window appears. If you are scanning a Windows NT/2000/XP/2003 machine, click on **Add Accounts**. For other machines, click on **Next** and proceed to Step 12**.**
Note: If you are logged in with a domain administrator account or with an account that has administrator rights to the machines that are being scanned, you do not need to **Add Accounts**, and can click **Next** and proceed to Step 12.



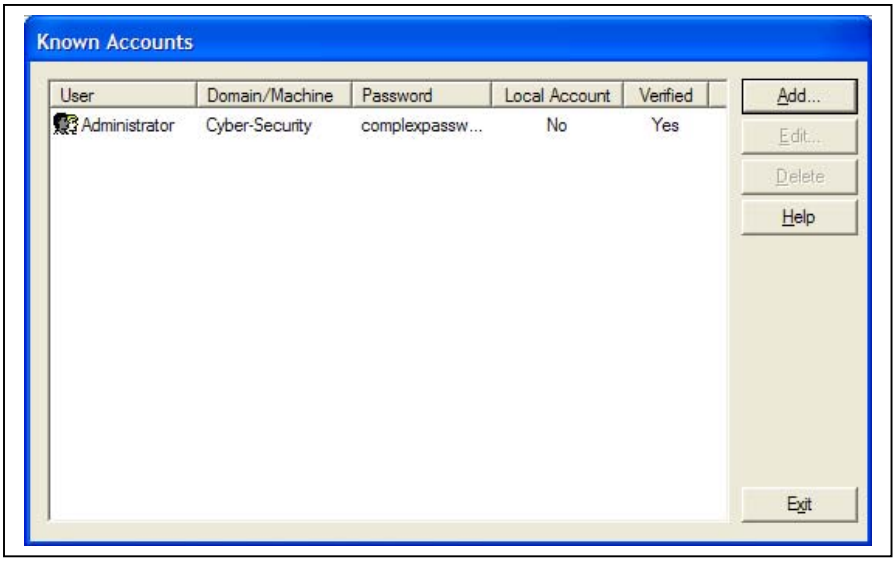
Step 8:
The Known Accounts window appears, click on **Add…**



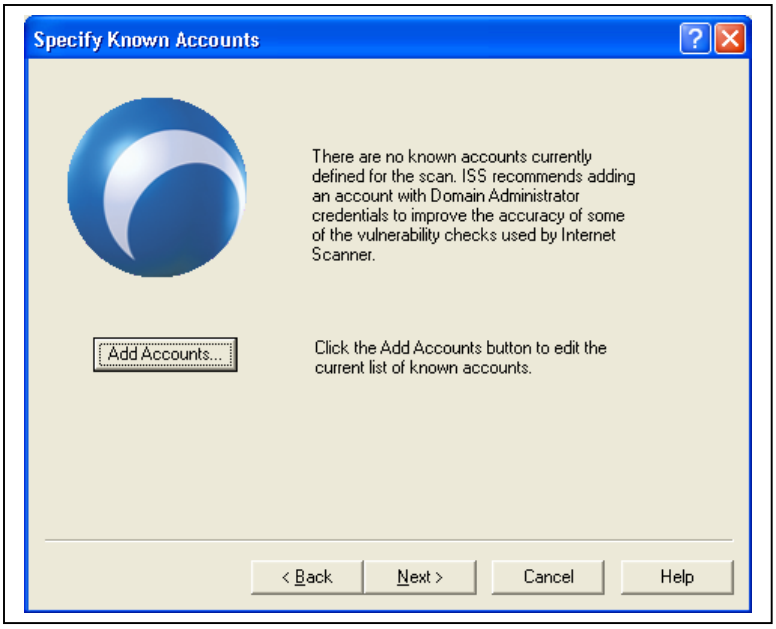
Step 9:
The Add Known Account window appears. Enter the **User Name, Domain Name, and password** of the administrator account to the machine being scanned. If you are using a local account, check local account, and type in machine name. Click on **Verified.** Click **OK** when finished.



Step 10:
The Known Accounts Window should show account credentials of the user you typed in. Repeat Steps 10 and 11 to add more accounts, or click **Exit** to end.

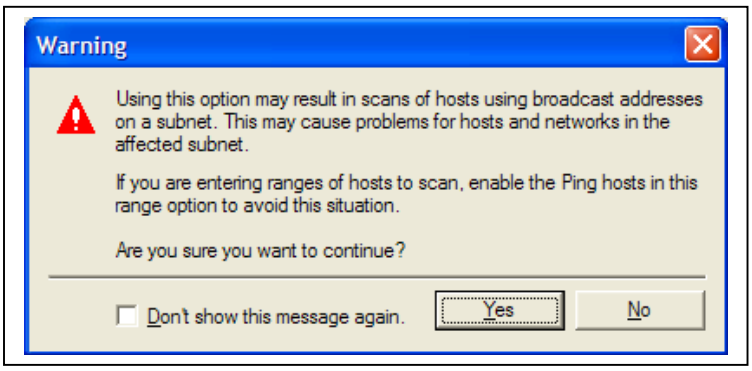


Step 11:
Click **Next** to continue.

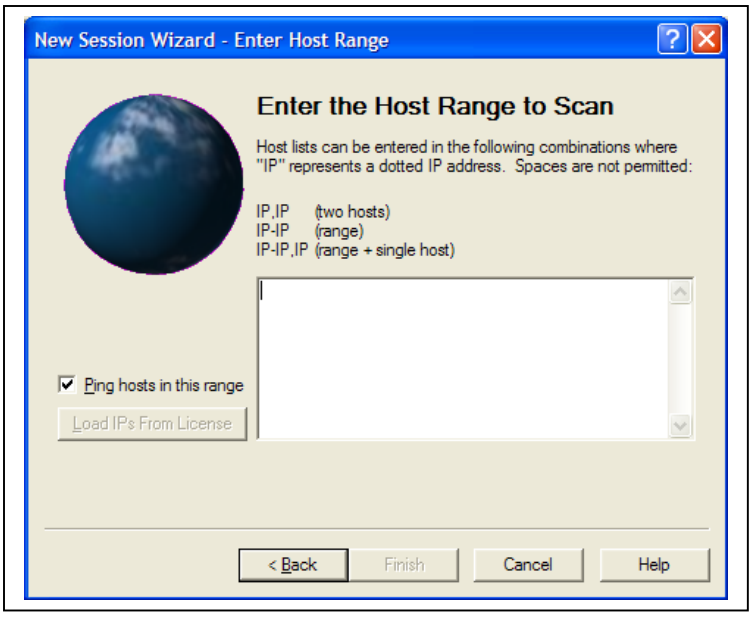


Step 12:
This screen chooses how the scanner determines which hosts to scan. Select **Enter Host Range** to manually choose your IP addresses, and Click **Next.**

Step 13:
You will get a warning banner indicating that this can cause unnecessary broadcast traffic on the network. Click **Yes** to continue.

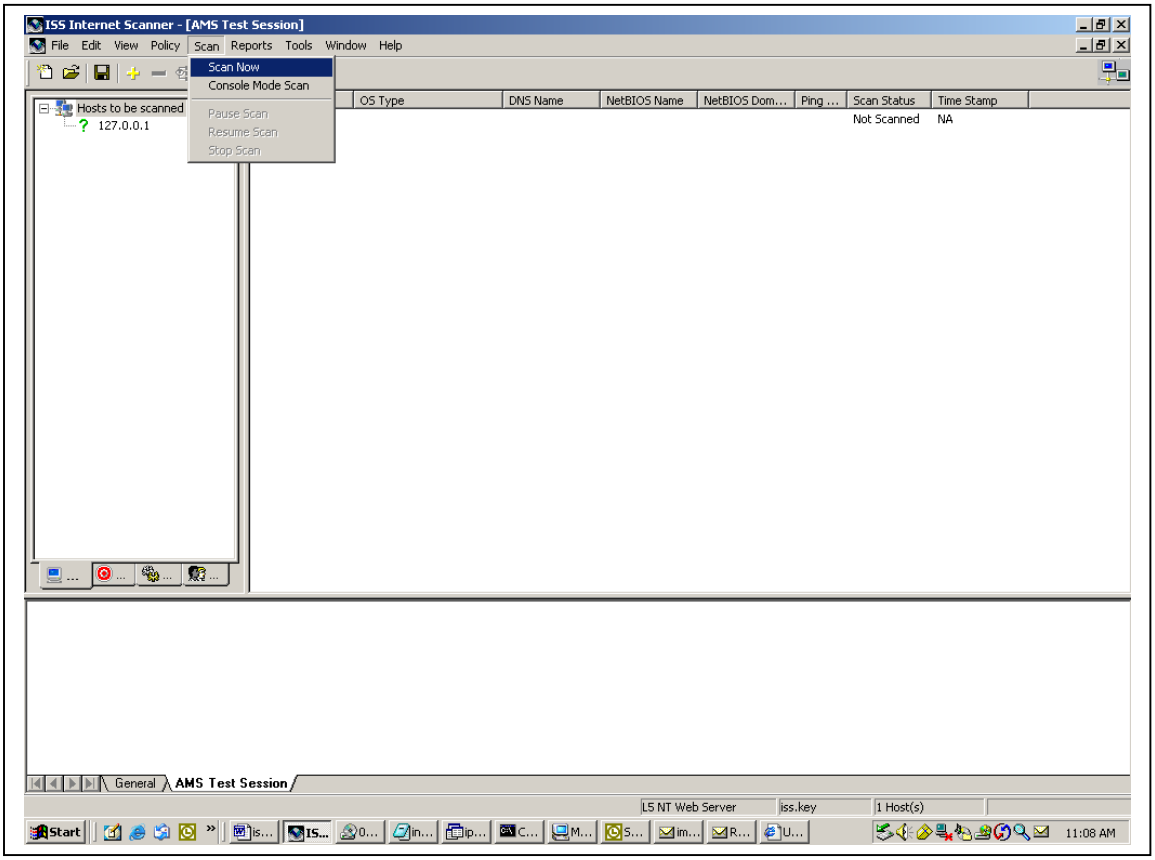


Step 14:
Type in the host range you wish to scan. When complete, Click **Finish**.

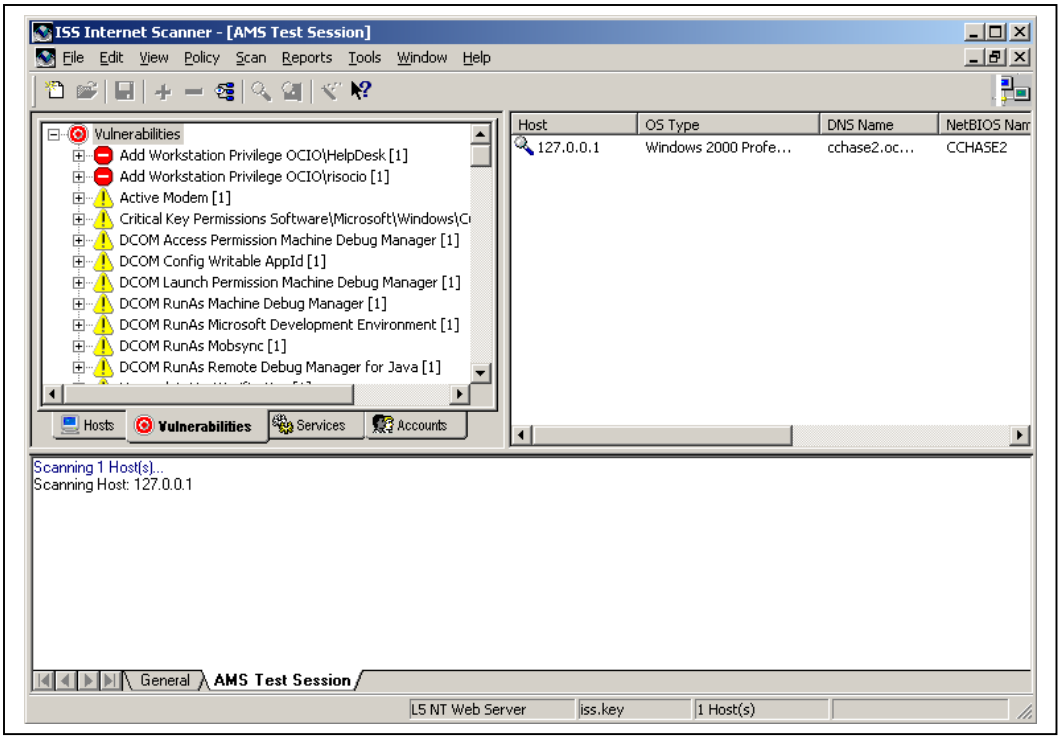


Note: USDA's intrusion detection system may record your scanning activities. Before you perform a scan, please send an email to scans@opsec.usda.gov indicating the IP addresses that you are scanning, as well as the IP address of the scanner. If possible, please provide 24 hours notice prior to performing a scan.

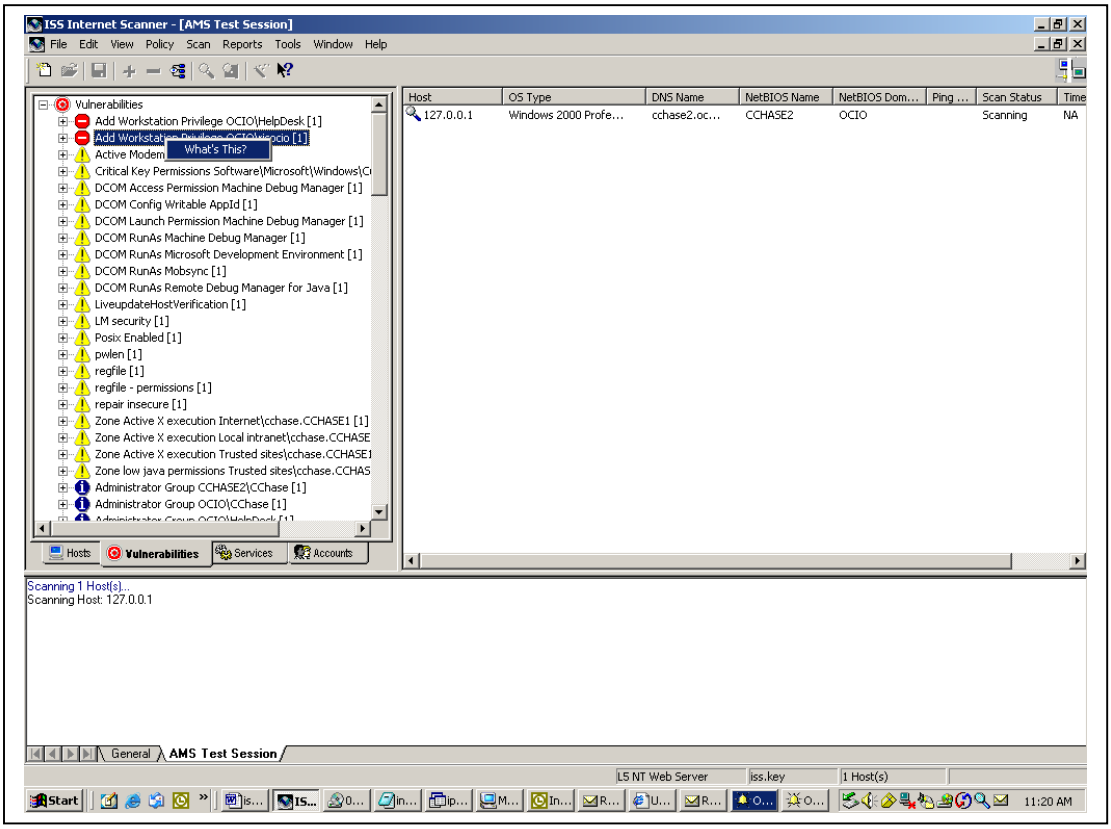
Step 15:
Internet Scanner will show the main scanner window. Click **Scan|Scan Now** to start the scan.



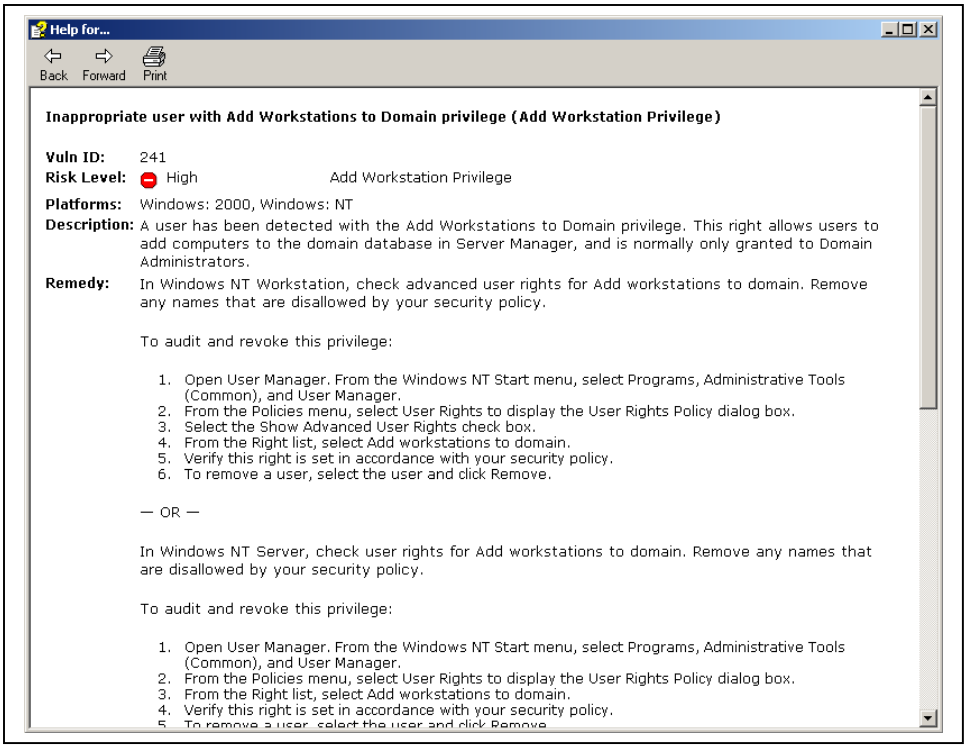
Step 16 (Optional): To view found vulnerabilities while scanning, Click on the **bullseye** vulnerability tab on the lower left frame.



Step 17 (Optional): To view details on the vulnerability, **Right Click** on the item and **Click** "What's This?"



Step 18 (Optional): The help window will appear with the details of your vulnerability.



Step 19: Once scanning has finished successfully, the results will be stored in Internet Scanner's database for retrieval at anytime.

Identifying Security Levels and Policies of Internet Scanner

Internet Scanner offers five levels of security that provide structured and logical approach to managing risk. These groups of security tests are applied to the systems. The higher levels are designed for business-critical systems; the lower risk levels are designed for less important systems. By applying these levels, you ensure that security efforts remain focused on the most important components of the IT infrastructure.

Security levels are types of checks that you apply to particular systems according to the amount of security needed. Level 5 is the most complex of the levels.

The following table lists each level and its description:

Level	Description
Level 1	Identifies operating systems of the machines on the network.
Level 2	Identifies the services running on machines on the network, such as web servers.
Level 3	Checks for compromises by unskilled attackers, or for signs that a system is already compromised.
Level 4	Checks for compromises by automated attack tools, or by moderately skilled attackers.
Level 5	Checks for compromises by highly skilled attackers, or for signs that a system is not configured properly.

Discovery Policies

Internet Scanner provides four default, read-only scan policies that gather operating system and service information about devices connected to the network.

Policy	Description
D0 Light Discovery	Provides a general idea of the types of devices and services active on the network. (DNS Lookups, ICMP, Fingerprinting)
D1 Standard Discovery	Runs processes that provide a general idea of the types of devices and services active on the network. (DNS Lookups, NetBIOS, Fingerprinting)
D2 Full Discovery	Gathers information about the network by performing port scans, operating system (stack) fingerprinting, banner grabbing techniques, and NetBIOS scans.

Policy	Description
D3 Maximum Discovery	Identifies any unknown or closed ports on devices connected to the network in addition to any database servers active on the network.

Assessment Scan Policies

Internet Scanner provides fourteen default, read-only scan policies that assess the security of devices connected to the network.

Policy	Description
Blank	Has no vulnerability checks enabled for the scan policy.
Evaluation	Runs vulnerability checks that detect the most extreme high and medium risk vulnerabilities, including all vulnerability checks performed by the SANS Top 20 policy. **Note:** All denial of service checks and some of the more time consuming checks included in Internet Scanner have been disabled in this scan policy.
Isdbs	Runs vulnerability checks that check for account names and passwords Database Scanner can use in gaining access to any database servers connected to the network.
L3 Desktop	Runs all high risk vulnerability checks to determine if a desktop connected to the network could allow an unauthorized user to: • gain immediate access to the system. • Gain superuser access • Bypass a firewall
L3 Router & Switch	Runs all high risk vulnerability checks to determine if a router or switch connected to the network could allow an unauthorized user to: • Gain immediate access to the system • Gain superuser access • Bypass a firewall
L3 Server	Runs all high risk vulnerability checks to determine if a server connected to the network could allow an unauthorized user to: • Gain immediate access to the system • Gain superuser access • Bypass a firewall

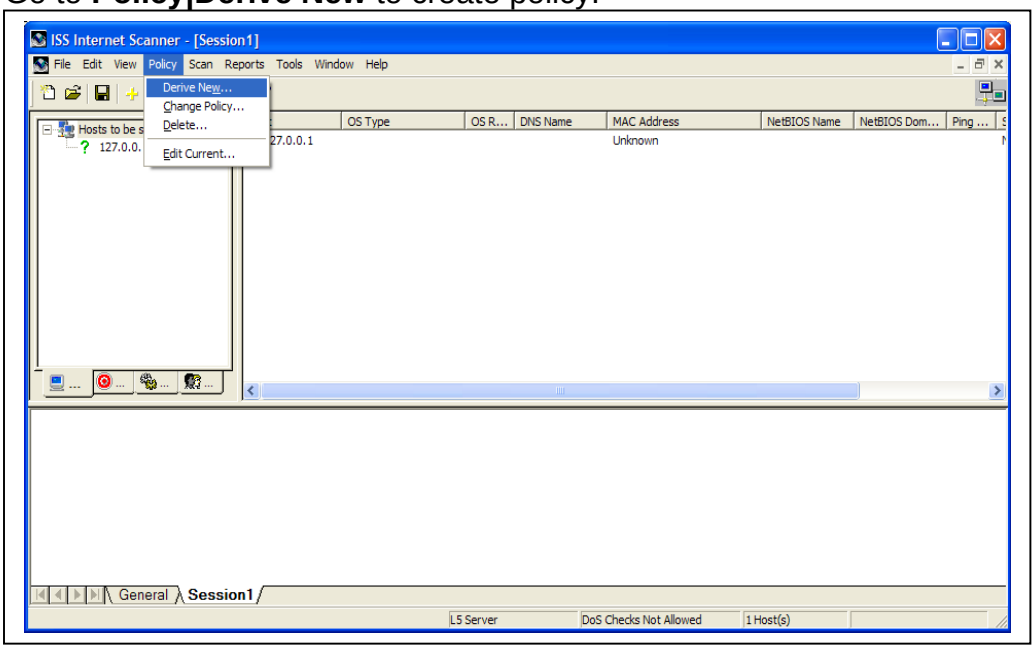
Policy	Description
L3 Web Server	Runs all high risk vulnerability checks to determine if a Web server connected to the network could allow an unauthorized user to: • Gain immediate access to the server by compromising the server through Web access methods (HTTP or CGI-BIN) • Gain superuser access • Bypass a firewall
L4 Router & Switch	Runs all high and medium vulnerability checks to determine if a router or switch connected to the network could allow an unauthorized user to gain system access to the network. **Note:** This scan policy also users the settings and vulnerability checks used by the L3 Router & Switch policy.
L4 Web Server	Runs all high and medium risk vulnerability checks to determine if a Web server connected to the network could allow an unauthorized user to gain system access to the network. **Note:** This scan policy also uses the settings and vulnerability checks used by the L3 Web Server Policy.
L5 Server	Runs all high, medium, and low risk vulnerability checks to determine if a server connected to the network could allow an unauthorized user to compromise or bring down the network. **Note:** This scan policy also uses settings and vulnerability checks used by the L3 Server policy and the L4 Server policy.
L5 Web Server	Runs all high, medium, and low risk vulnerability checks to determine if a Web server connected to the network could allow an unauthorized user to compromise or bring down the network. **Note:** This scan policy also uses the settings and vulnerability checks used by the L3 Web Server policy and the L4 Web Server policy.
L5 Max with Fusion	Combines L5 Server and L5 Web Server vulnerability checks, and adds any Fusion related checks not already included.
SANS Top 20	Runs the ten most common categories of exploits used against Unix system and the ten most common categories of exploits used against Windows systems. **Note:** See the SANS Web site and http://www.sans.org/top20 for more information on the SANS top 20 list.

Policy	Description
X-Force Catastrophic Risk Index Policy	Detects systems vulnerable to one or more of the most serious high-risk vulnerabilities and attacks listed in the X-Force CRI. See the ISS Web site at http://xforce.iss.net/xforce/riskindex for more information.

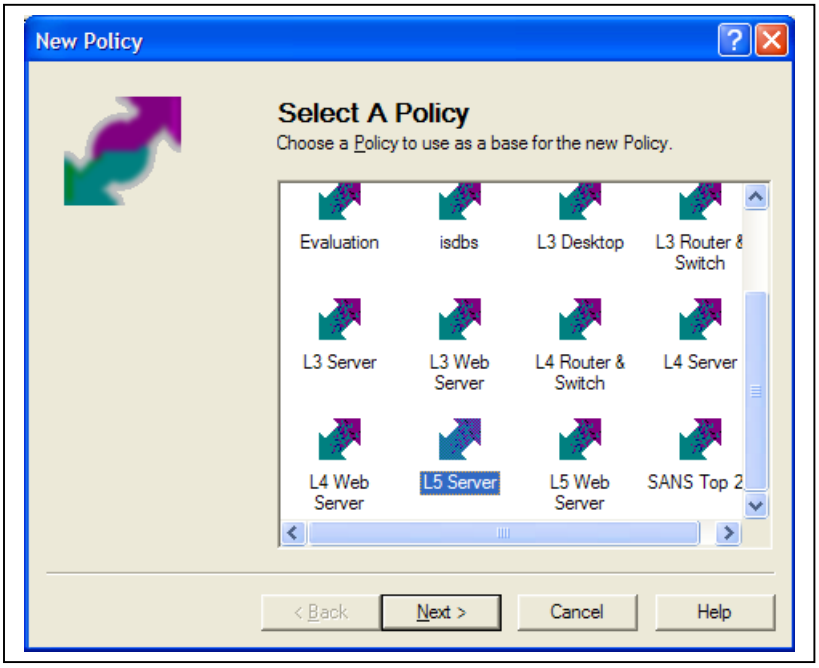
Editing Scan Policies

You can edit scan policies to scan for specific vulnerabilities or to turn off specific checks. The example below shows you how to create a L5 server scan that turns off brute force checks

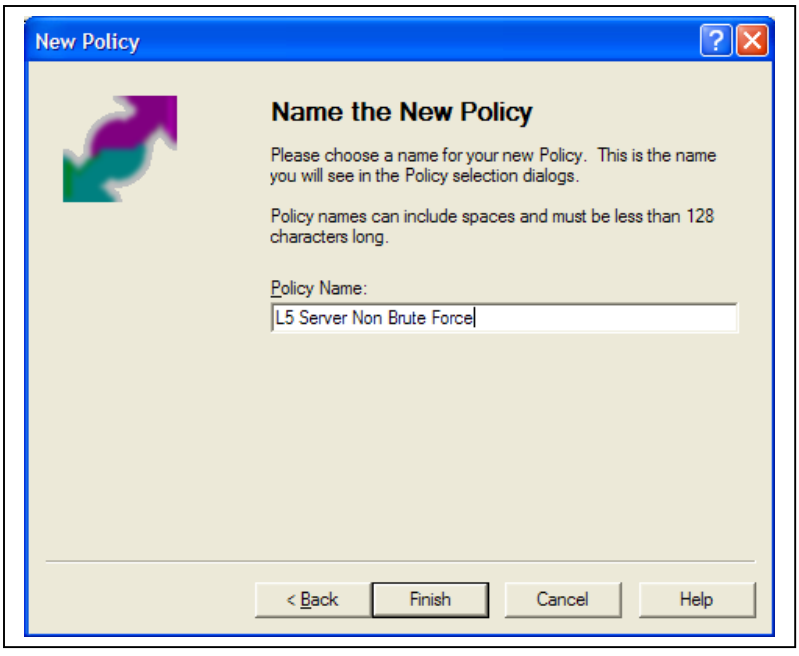
Step 1:
Go to **Policy|Derive New** to create policy.



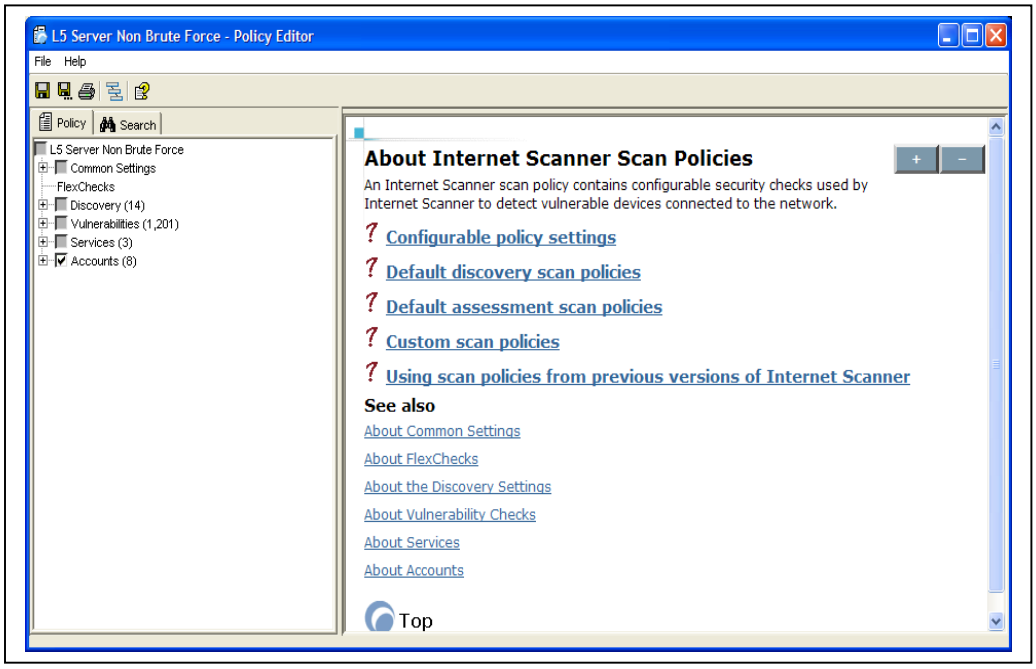
Step 2:
Select a policy to use a base for the new policy. In this case, we will select L5 Server. Click **Next** to continue.



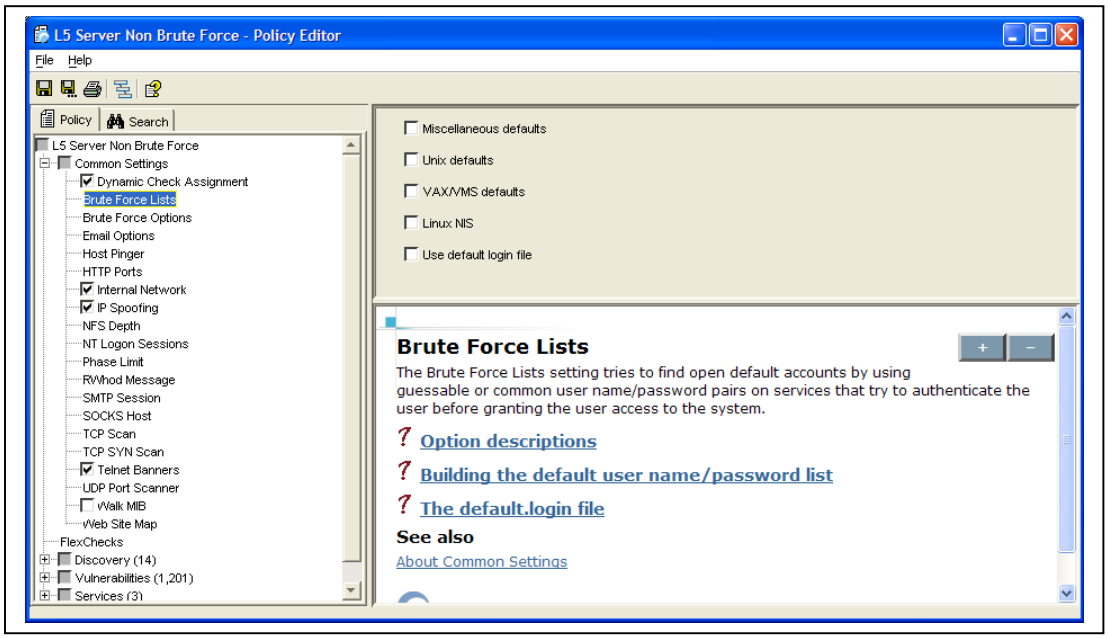
Step 3:
Create a name for the new policy. Click **Finish** when complete.



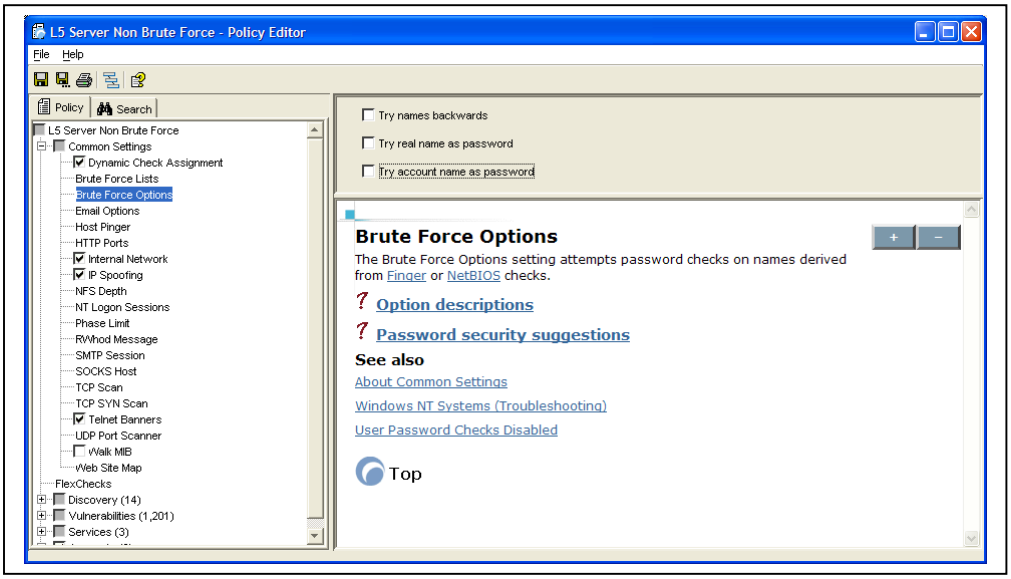
After finishing, the Policy Editor should appear.



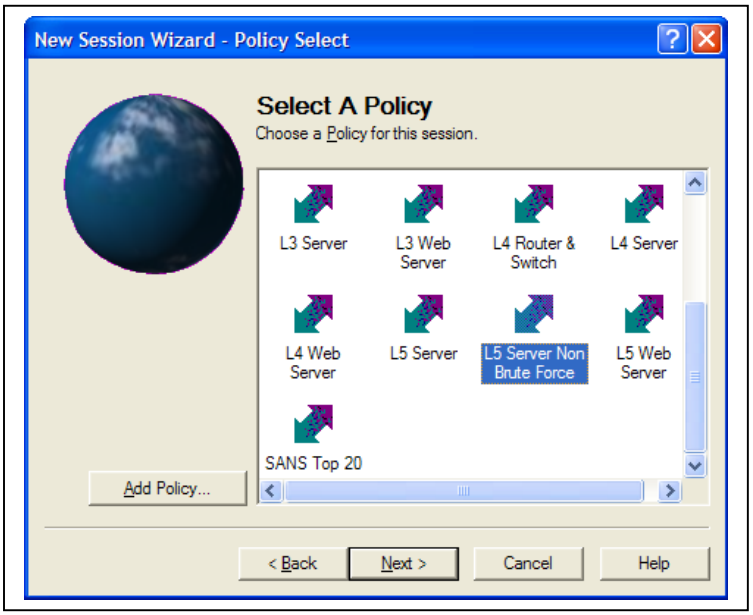
Step 4:
Expand “Common Settings” and click on Brute Force List. **Uncheck** all Operating System Checks in the right window.



Step 5:
Click on Brute Force Options. Uncheck all options in right window. When finished, click on the **save icon** or go to **File|Save**. When finished, click on the exit icon in the top right corner.



Your new policy will be listed the next time you configure a new scan session



Internet Scanning Reporting

About Reporting

Reports provide you the ability to view the results of the scan sessions. You can use reports to distribute information to people in your organization that can help correct the vulnerabilities**.**

Report Categories

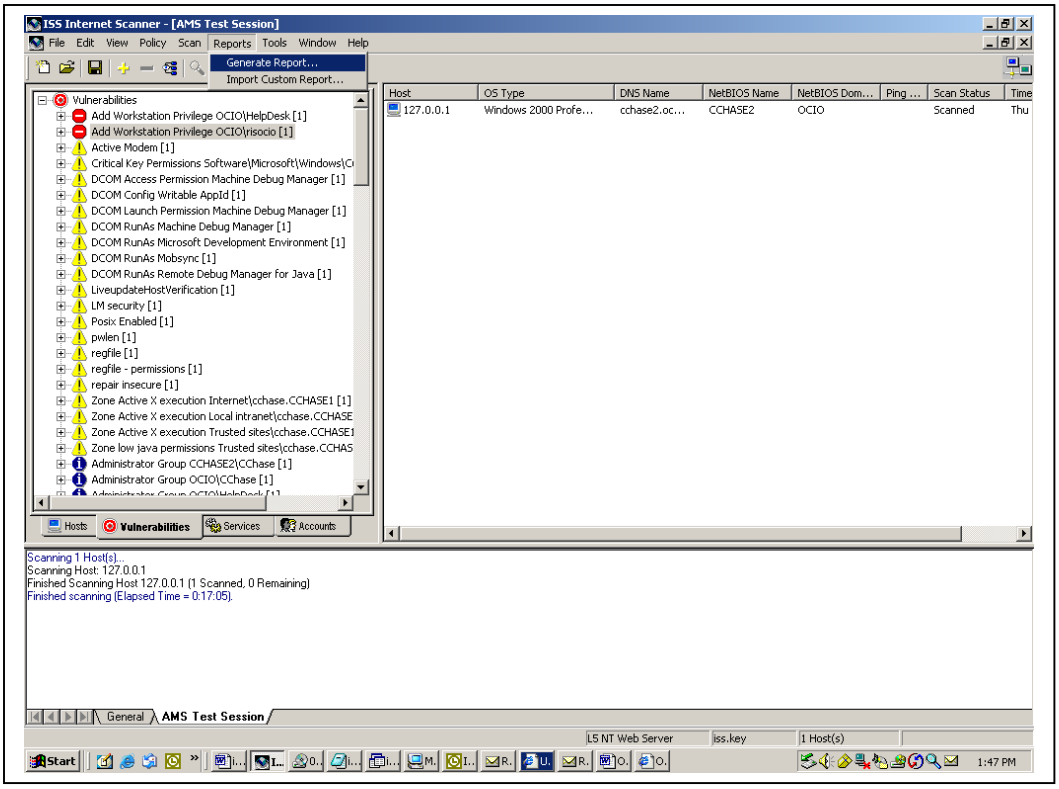
The reports are grouped into four categories to provide different levels of summary and detailed information. They are:

- **Executive** – provide summary information for speedy assessment of top-level security issues.
- **Line Management** – used for resource planning. Line management reports mainly show details of network scans
- **Technician** – provides the most detailed information on the status of your network. The descriptions are the same as the Line Management report. This information includes how to fix or patch vulnerabilities detected by Internet Scanner.
- **User Imported** – custom reports based on your own specification.

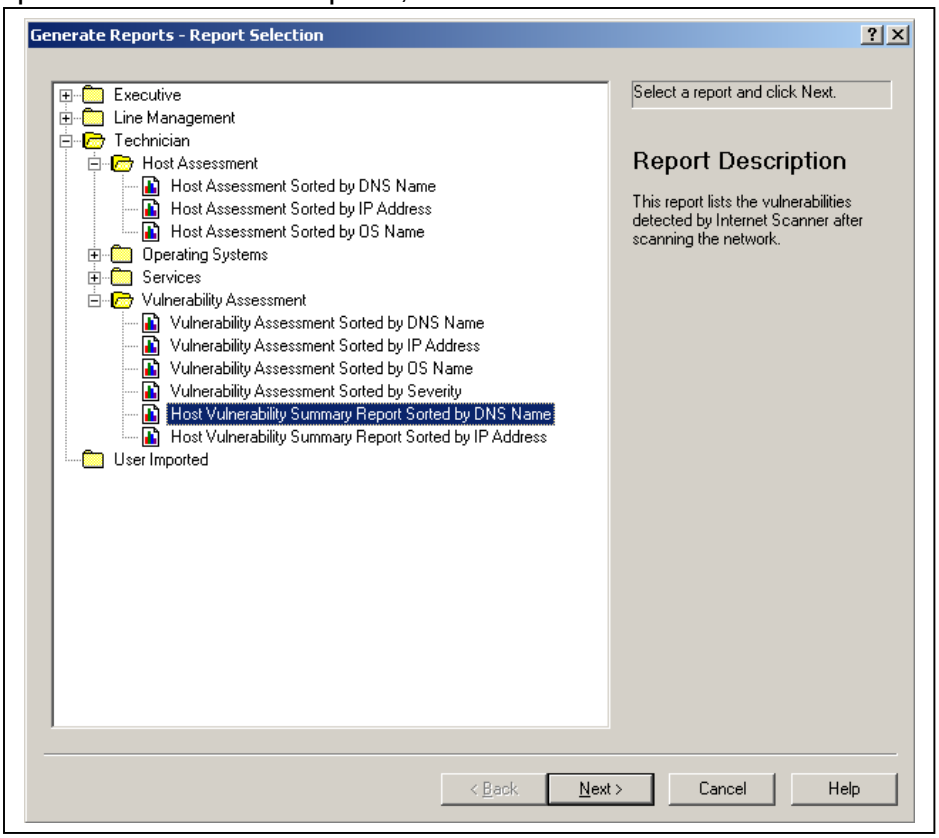
Generating a Report

Step 1: If Internet Scanner is not running, Click **Start|Programs|ISS|Internet Scanner 7.0 |Internet Scanner 7.0.** If Session wizard appears, Click **Cancel**.

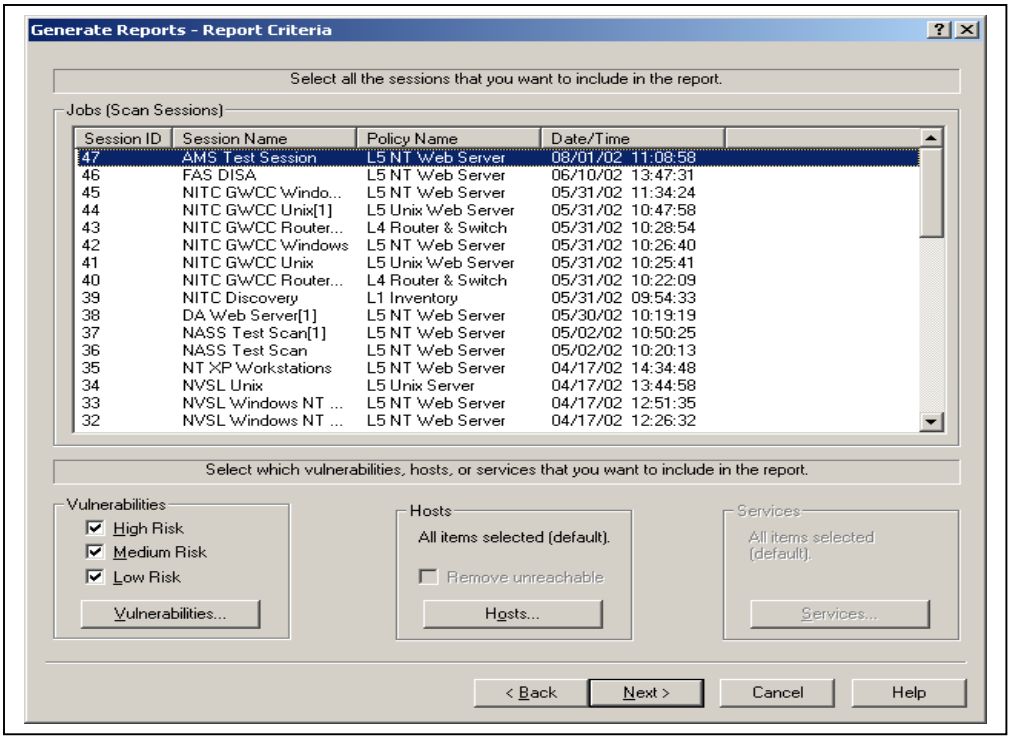
Step 2: Click on **Reports|Generate Report**



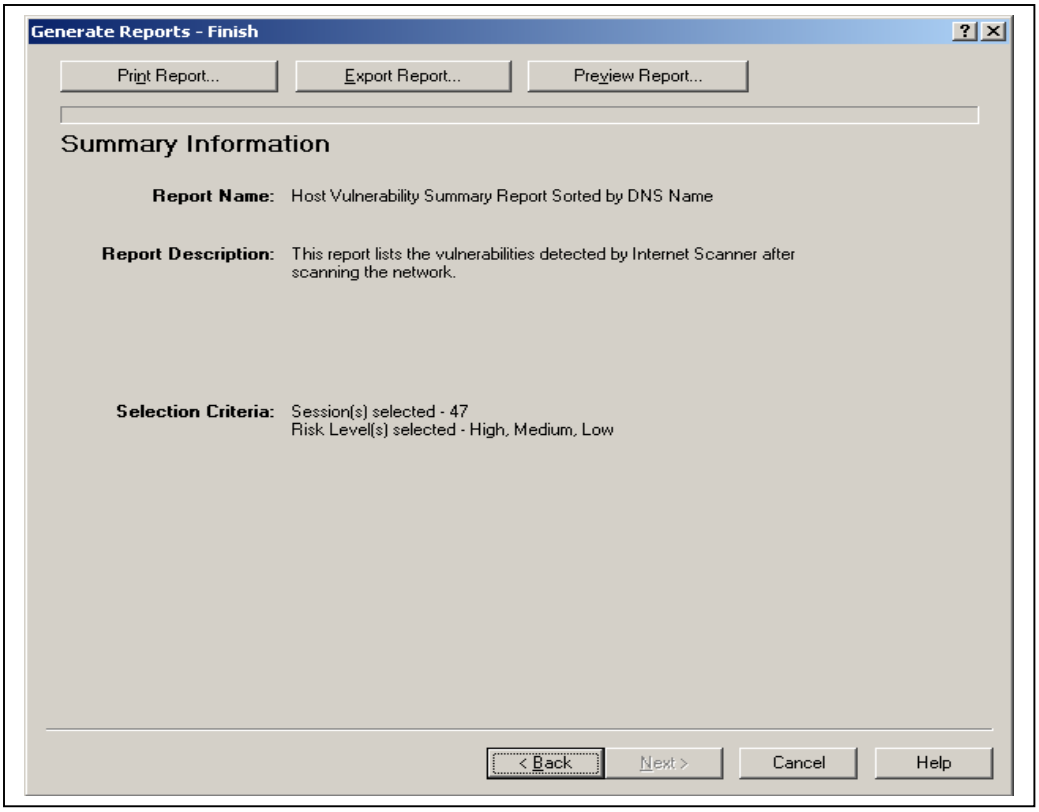
Step 3: From Report Selection, **Select** the type of report that you wish to run. For a description of Technican Reports, see the next session. Click **Next**.



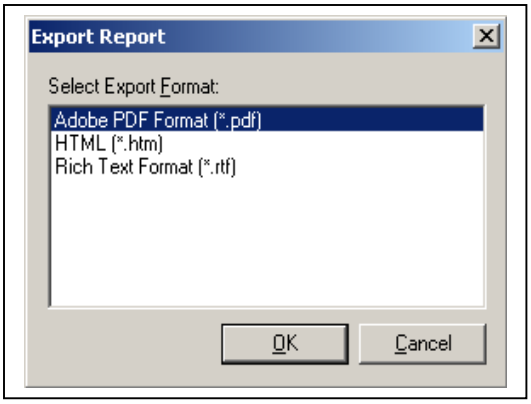
Step 4: Select the session and vulnerabilities that you want to include in this report. Click **Next**.

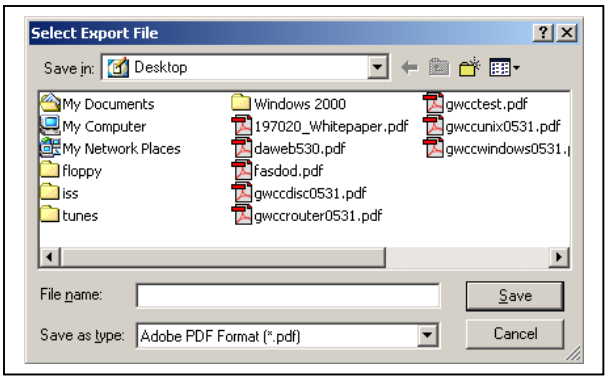


Step 5: Select **Print Report, Export Report or Preview Report** to get desired results, for this purpose, we will select Export Report.



Step 6: Select format, and then **OK**. The Select Export File window will appear. **Select** a name and then **Save** to save the report.





Technican Vulnerability Assessment Reports

For Systems Administrators, the most important reports are the Technician Vulnerability Assessment Reports, as they give the most detailed information about vulnerabilities that were found on a particular system. All of the reports in this section gives the same vulnerability details and summaries.

Archiving of Reports in Accordance to Federal Law

Federal laws require agencies to retain records and documents associated with IT systems, which includes Internet Scanner. Please be aware that Internet Scanner will generate records that must be retained according to Federal guidelines. For more information on records management, please contact your Records Officer, or visit the National Archives at:
http://www.archives.gov/records_management/ardor/grs24.html.

Scheduling Internet Scanner

Internet Scanner provides the capability to run Internet Scanner at specific times during the day. However, there is no graphical user interface to schedule scans, and you must use the Command Line Interface/Engine Manager along with Windows Scheduler to schedule Internet Scanner events. The example below shows how you can schedule Internet Scanner to run a scan at a specific time.

Step 1:
Go to command prompt. At command prompt, change directory to **c:\program files\iss\scanner console**.

```
C:\>cd c:\program files\iss\scanner console

C:\program files\iss\scanner console\>
```

Step 2:
Once at the proper directory, you must use the "Addasset" command under engine manager to add the Internet Scanner sensor before you can use any other command line interface for the sensor. Type the following two syntax entries at the command line and hit enter. Replace "cchase" with your computer name. Replace "scanner_1" with your sensor name. You should receive a successful command after the second syntax command.
NOTE: This needs to be performed every time you reboot your machine. You can also create a batch file to perform this command.

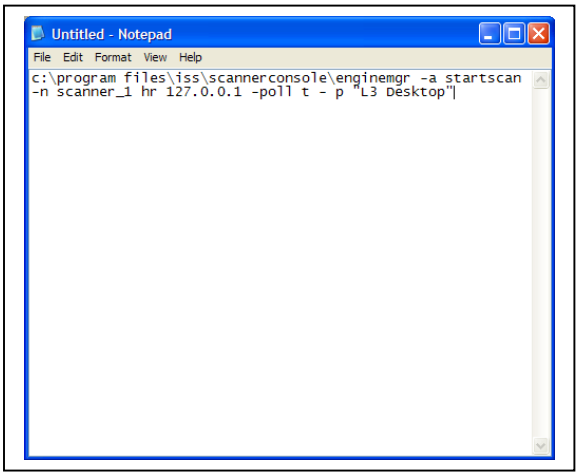
```
C:\Program Files\ISS\ScannerConsole>EngineMgr -a addasset -e cchase -n scanner_1 -t
scanner -o stdout.txt

C:\Program Files\ISS\ScannerConsole>EngineMgr -a addasset -e cchase -n scanner_1 -t
scanner -mp EngineMgr.policy

AddAsset for scanner_1 at 199.128.144.92 completed successfully
```

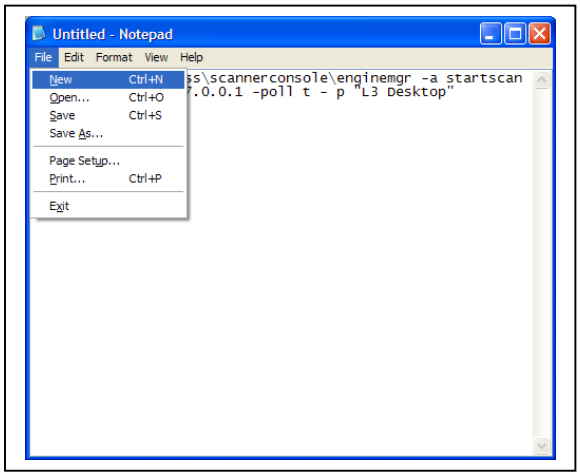
A description of the syntax commands for EngineMgr used in this example is on page 49.

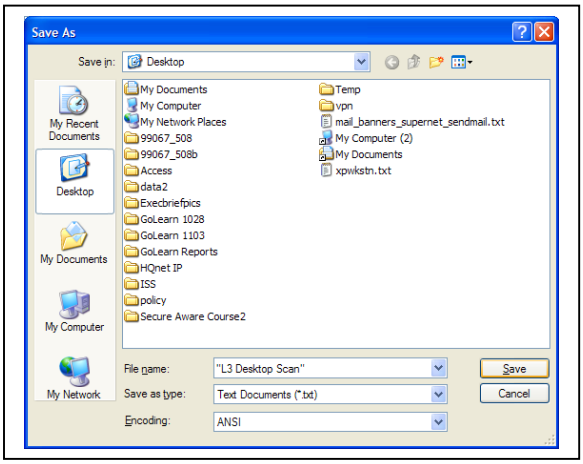
Step 3:
You will need to create a batch file to schedule the automated session. Open Notepad and type the following syntax.

```
c:\program files\iss\scannerconsole\enginemgr -a startscan -n scanner_1 -hr
127.0.0.1 -poll t -p "L3 Desktop"
```

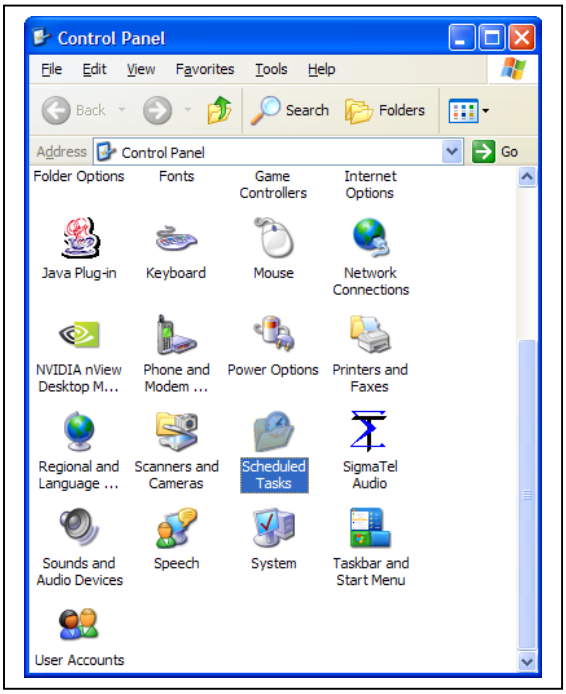
Step 4:
Save the file as a unique file name with the extension of ".bat" in a specified directory. Be sure to use double quotes when you are saving. After saving, exit out of Notepad.



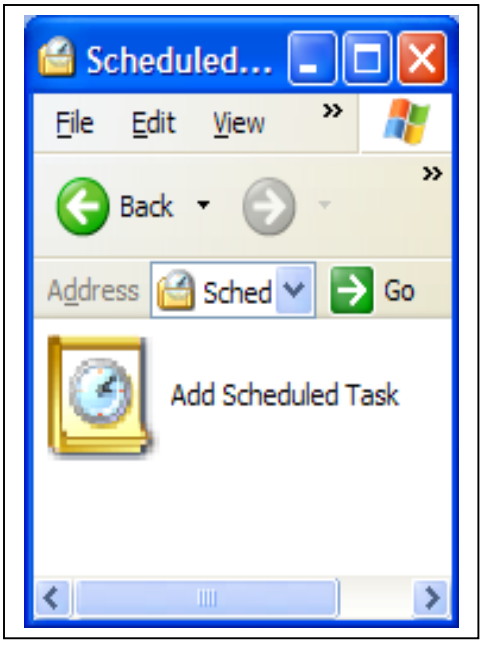




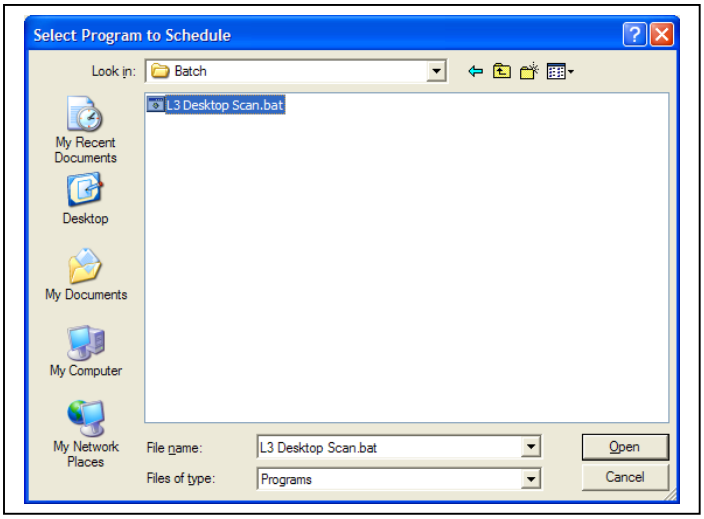
Step 5:
Go to Start|Settings|Control Panel, and open scheduled scans



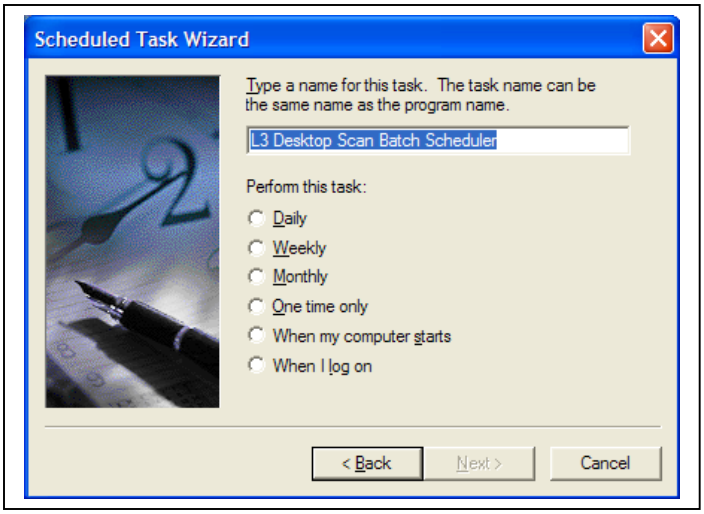
Step 6:
Click Add Scheduled Task.



Step 7:
Under Select Program to Schedule, Select Batch file created in Step 4. **Click** Open.



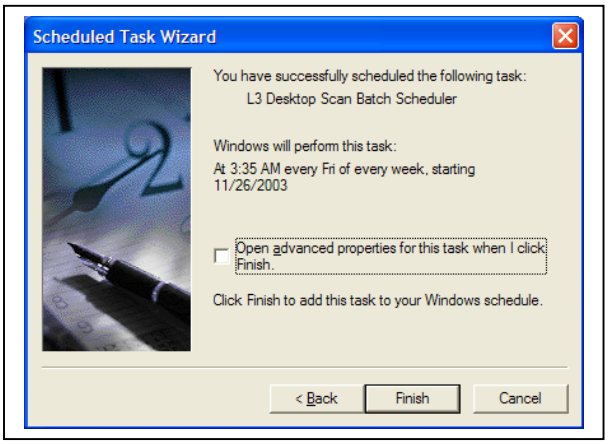
Step 8:
Type a name for this task. Select when to perform this task and **click** Next.

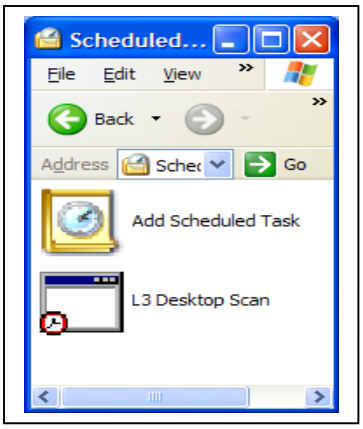


Step 9:
Select the day and time you want to perform this task. **Click** Next.

Step 10:
Under "Enter the name and password of a user", you must enter a user ID with local administrator rights to the machine. **Click** Next when done.

Step 11:
Click Finish when complete. You should see your newly scheduled task in the Scheduled Scans window.





EngineMgr Common Syntax Commands

Option	Description
-a	The action performed by the Internet Scanner sensor. Default: none
-e	The IP address where the Internet Scanner sensor resides. This option is not used for the help and version commands, but can be used with all other CLI commands. Default: 127.0.0.1
-hf	Specifies a host file to be used. File listed by be in quotes.
-hr	A comma and/or hyphen separated list of IP addresses specifying the range of hosts to scan
-mp	The file name of the Engine Manager policy file. This option can be used with all CLI commands Default: EngineMgr.policy
-n	The name of the Internet Scanner sensor. Default: scanner_1
-o	The complete name and file path of the output file. This option can be used with all CLI commands. Default: stdout
-p	The file name of the policy file
-t	The engine type

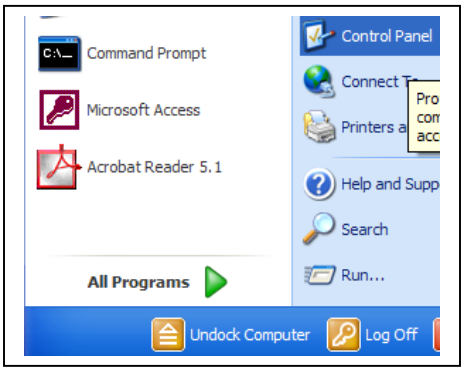
A complete list can be found in the “Internet Scanner User’s Guide”, by ISS.

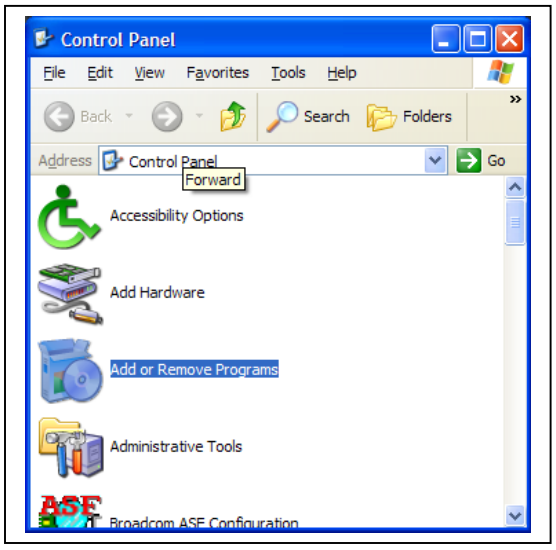
Removing and Uninstalling Internet Scanner

These instructions show you how to uninstall Internet Scanner and MSDE from a standard installation If you have multiple instances of MSDE installed or are running any other ISS product such as Site Protector, please contact ISS or Microsoft technical support before following these instructions.

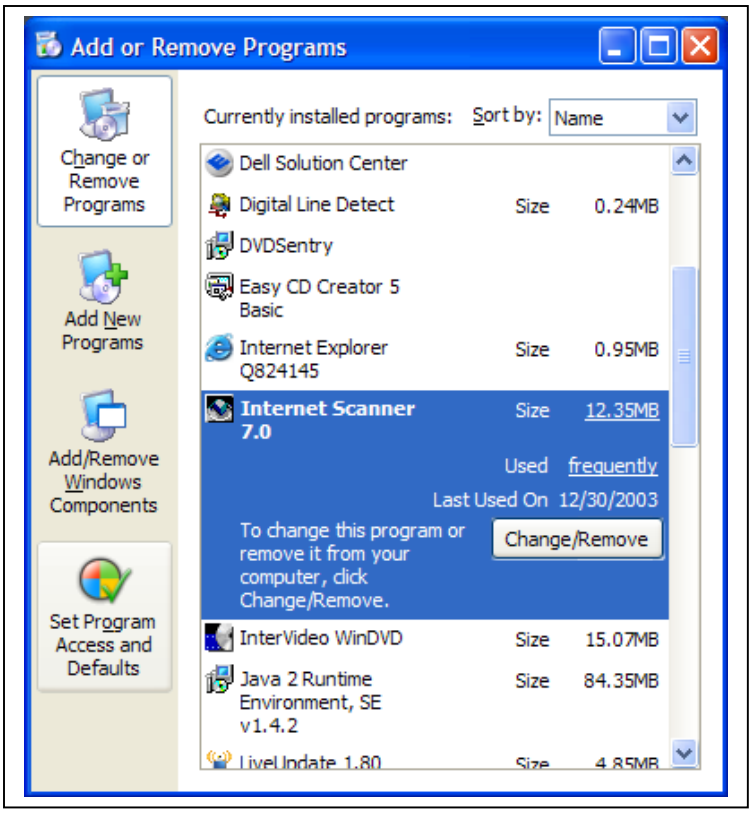
WARNING: These instructions contain information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Use Registry Editor at your own risk.

Step 1:
Click on Start|Control Panel and **click** on “Add and Remove Programs”.



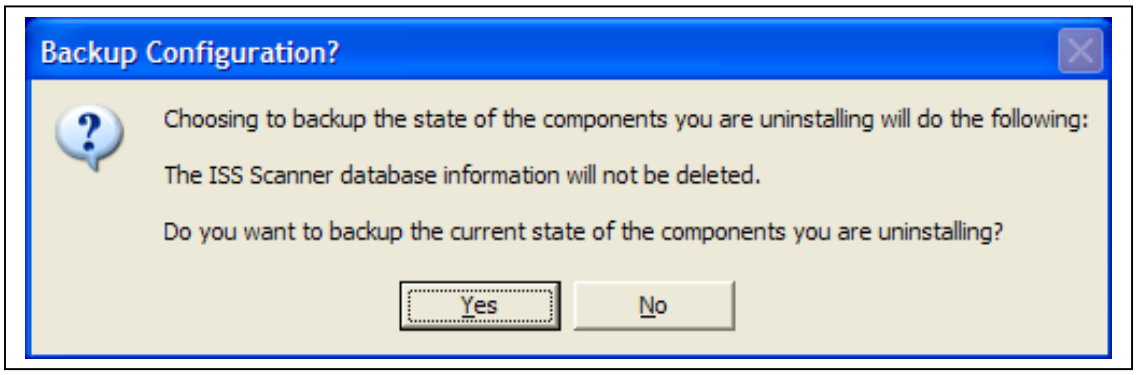


Step 2:
The Add/Remove Programs Window appears. **Highlight** Internet Scanner 7.0 and **click** Change/Remove.

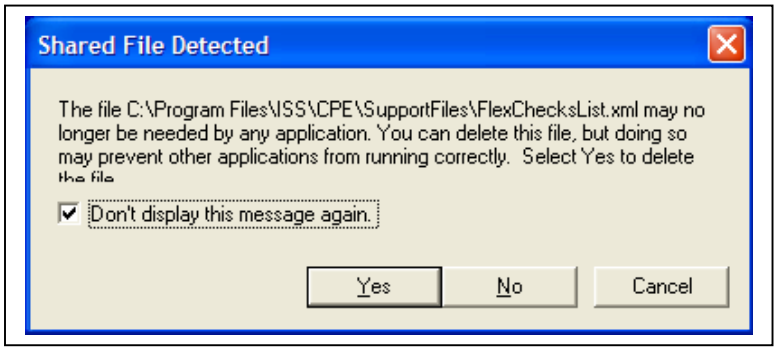


Step 3:
An uninstall dialog box appears asking: "You have chosen to uninstall an ISS component. Cryptographic keys will not be removed from the system during uninstall. Are you sure you want to uninstall?" **Click** Yes.

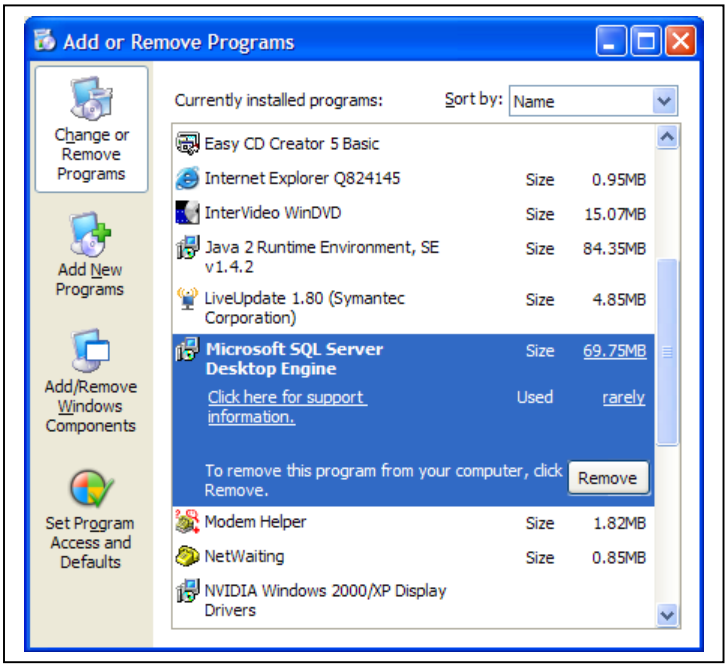
Step 4:
The Backup Configuration dialog box appears asking: "Choosing to backup the state of components you are uninstalling will do the following: The ISS Scanner database information will not be deleted. Do you want to backup the current state of the components you are uninstalling?" **Click** No.



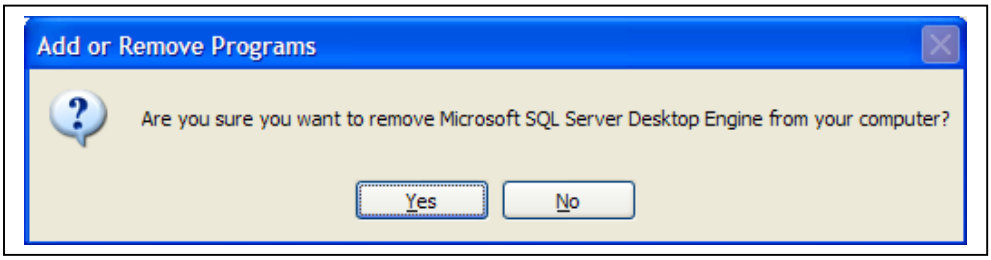
Step 5:
The Shared File Detected dialog box appears. Click "Don't display this message again" and **Click** Yes to delete this file. This dialog box may appear several times during the uninstall. Internet Scanner should uninstall successfully.



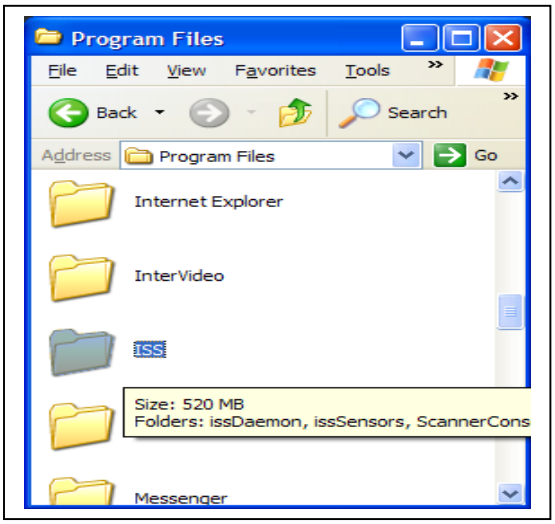
Step 6:
Go back to the Add/Remove Programs Window. **Highlight** Microsoft SQL Server Desktop Engine and **click** Remove.



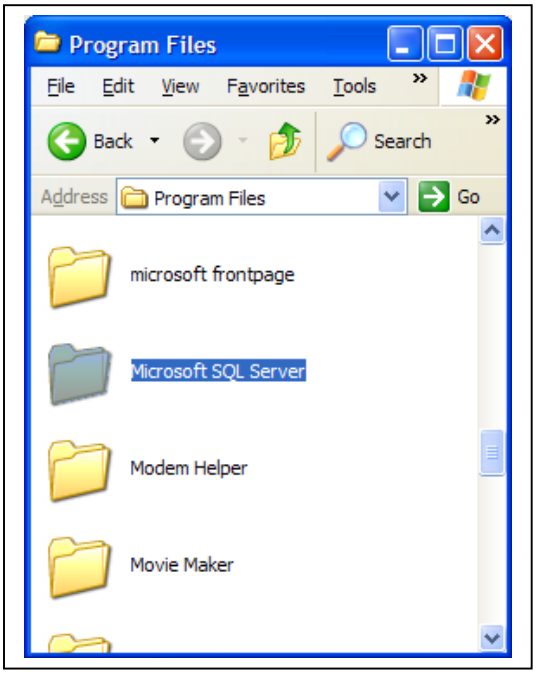
Step 7:
The Add Remove Programs dialog box appears asking: "Are you sure you want to remove Microsoft SQL Server Desktop Engine from your computer? **Click** Yes. MSDE should uninstall successfully. When finished, close out of Add/Remove Programs.

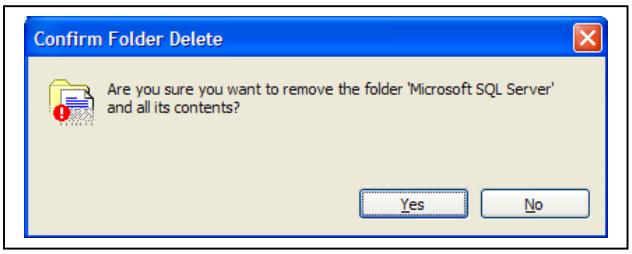


Step 8:
Using Windows Explorer, **navigate** to the C:\Program Files directory. Highlight the ISS Directory and **press** the delete key. **Click** Yes to remove ISS and all its contents.

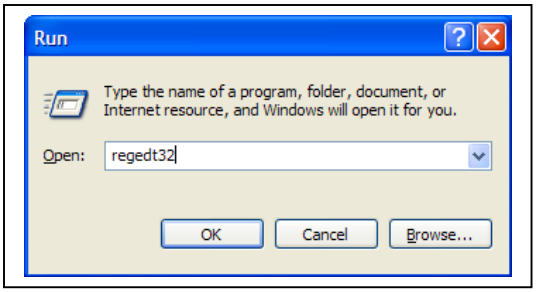


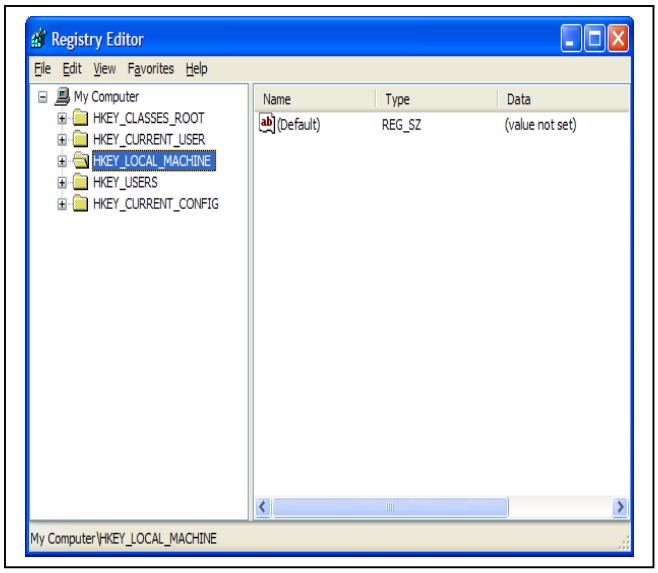
Step 9:
Under C:\Program Files, highlight the Microsoft SQL Server directory and **press** the delete the key. **Click** Yes to remove Microsoft SQL Server and all its contents.



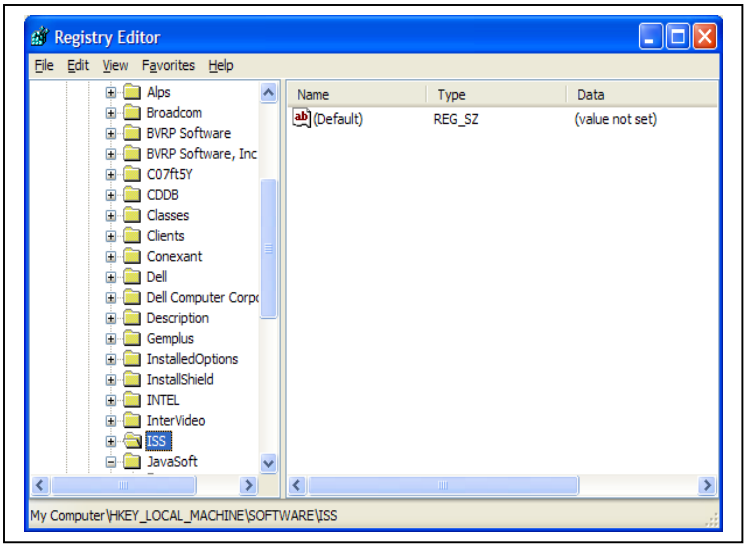


Step 10:
Click on Start|Run and **type** Regedt32. The registry editor should appear.

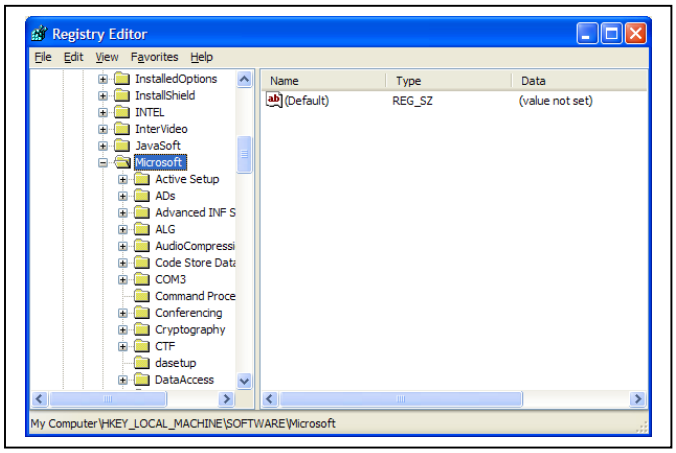


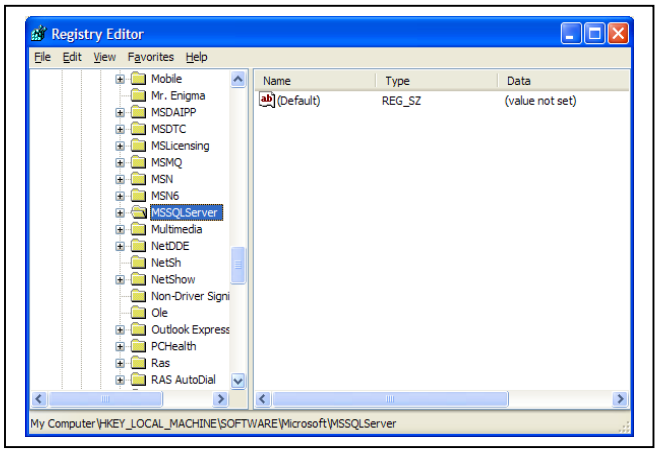


Step 11:
Expand the HKEY_LOCAL_MACHINE hive and **navigate** to HKEY_LOCAL_MACHINE|SOFTWARE until you find the ISS key. Highlight the ISS key and **press** delete key to delete to remove key and all subkeys.



Step 12:
Navigate to HKEY_LOCAL_MACHINE|SOFTWARE|Microsoft| until you find the MSSQL Server key. Highlight the MSSQL Server key and press delete to remove key and all subkeys.





Step 13:
When finished, exit out of Regedt32 and reboot machine. Internet Scanner and MSDE should be fully removed.

For more information on removing MSDE, please see the Microsoft Knowledge Base article 290991 entitled “HOW TO: Manually Remove SQL Server 2000 Default, Named, or Virtual Instance” at the link below.
http://support.microsoft.com/default.aspx?scid=kb;en-us;290991&Product=sql2k

Appendix B
USDA Monthly Scan Certification

Agency_____ **ISSPM Name**_____

1. Number of Devices Scanned in the Past 30 Days_____

2. Do these devices include all systems and desktops? Yes_____ **No**_____

2a. If no, please include an explanation to include target dates when all systems and desktops will be scanned.

3. Were vulnerabilities (excluding false positives) found? Yes_____ **No**_____

4. Have all vulnerabilities been mitigated? Yes_____ **No**_____

4a. If not, have Plan of Action and Milestones (POA&M) been created and reported under the Federal Information Security Management Act (FISMA) to address these vulnerabilities? Yes_____ **No**_____

Certification Signature:

_____ _____

Name **Date**